Data and Consent Issues with Neural Recording Devices

11

Stephen Rainey, Kevin McGillivray, Tyr Fothergill,
Hannah Maslen, Bernd Stahl, and Christoph Bublitz

Contents

Abstract

Research-driven technology developments in the neurosciences present interesting and potentially complicated issues concerning data in general and, more specifically, brain data. The data that is produced from neural recordings is unlike names and addresses in that it may be produced involuntarily, and it can be processed and reprocessed for different aims. Its similarity with names, addresses,

S. Rainey (✉)
Oxford Uehiro Centre for Practical Ethics, University of Oxford, Oxford, UK
e-mail: stephen.rainey@philosophy.ox.ac.uk

K. McGillivray
University of Oslo, Oslo, Norway

T. Fothergill · B. Stahl
De Montfort University, Leicester, UK

H. Maslen
University of Oxford, Oxford, UK

C. Bublitz
Faculty of Law, University of Hamburg, Hamburg, Germany

etc. is that it can be used to identify persons. The collection, retention, process-ing, storage and destruction of brain data are of high ethical importance. In terms of policy, as one strand of a broader fabric of measures to cope with this, we can ask: is current data protection regulation adequate in dealing with emerging data concerns that relate to consumer neurotechnology and consent?

11.1   Questions and Scope

This chapter provides an overview of some of the sorts of question that might arise from a data protection perspective as they relate to consent in the use of brain-computer interfaces. This ought to aid in promoting a better understanding of these technologies from a potential consumer perspective, especially by discussing vari-ous possibilities for recording and processing brain signals, which are likely to appear in consumer technologies. Highlighting these common areas of concern for consumers will provide product developers with insight into the context that their products will be used in. This is important for consumers to whom the products will be marketed, and to the regulatory frameworks that will most likely constrain the functions of these products. Moreover, brain-signal recordings that are generated from direct to consumer (DTC) devices provide data of an indeterminate type (is it personal data, medical data?). Discussion of these issues is required to bring neuro-data issues to the attention of policymakers.

At least two relevant points concerning data and consent emerge in cases of neu-ral recordings:

1. Recording: While a user can easily consent to using a device to record data for specific purposes, recording involuntary data may occur without user consent.
2. Processing: What does processing data entail and does this have ramifications for consent?

Informed consent has a long heritage as a sine qua non for human research. It forms part of good clinical practice and is enshrined as such in the European Commission Directive 2001/20/EC, which describes the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use:

Informed consent is the decision, which must be written, dated and signed, to take part in a clinical trial, taken freely after being duly informed of its nature, sig-nificance, implications and risks and appropriately documented, by any person capable of giving consent or, where the person is not capable of giving consent, by his or her legal representative; if the person concerned is unable to write, oral con-sent in the presence of at least one witness may be given in exceptional cases, as provided for in national legislation.[1]

The broader policy position on informed consent appears in the Declaration of Helsinki, referencing the necessity of ethical considerations:

---

[1] The full directive can be viewed at https://ec.europa.eu/health/human-use/clinical-trials/direc-tive_en [accessed March 2019].

The design and performance of each research study involving human subjects must be clearly described and justified in a research protocol. The protocol should contain a statement of the ethical considerations involved and should indicate how the principles in this Declaration have been addressed.[2]

Before going on to treat these issues in terms of consent, some limitations need to be established. First, we will limit ourselves to examining data in terms of the European General Data Protection Regulation (GDPR) [1].[3] This limitation is advisable owing to its scope, the authors' familiarity with it and the availability of space that precludes a more widespread treatment. Second, we will not engage in a detailed legal analysis of contract law and consumer law where 'consumer BCI devices' are mentioned. One reason for this is lack of space. Another is the future-facing nature of the technology under scrutiny. We wish to maintain a higher level of analysis so that we can anticipate ethical concerns that may be on or beyond the horizon. By operating at this level, we will be able to maximise the scope and applicability of our analysis.

11.2 How Neurotechnologies Work

Neurotechnologies typically work by reading, recording and processing brain signals. In research contexts, the process of recording permits various degrees of invasiveness from scalp-based electroencephalogram (EEG), brain surface electrode (electrocorticography, or ECOG) arrays to intracortical probes. Consumer contexts tend to use scalp-based type EEG approaches, for obvious reasons. These can be used to operate different types of devices including wheelchairs, prosthetic limbs, drones or software programs. They can be put to use for rehabilitation, or sometimes as means of neuro-optimisation and enhancement by providing users with feedback on their neural activity [2–5]. The therapeutic potential of these approaches is tantalising, in allowing individual, brain-based ways to overcome problems in mobility, affective disorders, cognitive impairment, or in fine-tuning brain processes according to will. But the idea of 'mind'-controlled devices is more widely seen as an interesting and exciting mode of engagement with technologies for consumer applications or creative pursuits [6–12]. Does the nature of neural recording, processing and modulating pose a potential risk in terms of consent and how the data derived from brains is used?

There is increasing public understanding about issues surrounding consenting to online data collection and use [13, 14]. Yet, there still remains much complacency and ongoing misuse of these data [15]. Many major technology companies have been implicated in over-reaching with their data collection activities. The consequences for the public have included reputational damage to political systems following microtargeted voter swaying campaigns, as in the 2016 UK Brexit referendum [16, 17]. These are issues that may potentially have far-reaching consequences and implications.

---

[2] World Medical Association, 2000, paragraph 22, describes the context for informed consent http://www.wma.net/en/30publications/10policies/b3/ [accessed March 2019].

[3] Subsequent references to specific parts of GDPR legislation refer to the English language version of the regulation.

Social media companies that enable this kind of activity have reportedly seen user activity change. While user numbers have fallen in general, greater awareness of privacy-impacting conditions on such platforms has resulted in changing attitudes towards participation, as well as changing attitudes towards privacy itself [18–20]. Political concern and media attention have focussed on slow responses to dealing with data problems [21, 22]. While a lot of data obtained by social media companies and others is given voluntarily (if not advisedly), more data than is sometimes realised is obtained by obfuscated means. A wide variety of data can be collected without the express knowledge of the user, and thus only with a very dubious sense of their 'consent' (See for instance [23]). Inferences can be drawn about user activity in general, based upon data derived from what kind of web history a user has, for example, or from their location data as recorded while using the internet from a mobile phone. This provides a clear parallel with brain-signal recording that is worth drawing out.

11.3   Neural-Signal Recording

Neural data has multifarious uses in research contexts to indicate memory content, motor and speech intention, mood and educational aptitude, among other things. As such, this represents data that could easily be framed as sensitive, personally identifying and revelatory about a person. This is made all the more acute by the growing market in consumer neurotechnology. Although neural data is mostly collected for medical and neuro-science research, the recent increase in digital health technologies beyond research and medical facilities to non-invasive and readily accessible consumer-grade applications raises issues of privacy and informed consent. If we are unprepared, or underprepared, in dealing with online data collection and use, we ought to be bracing for the potential risks inherent with neural data collection, as this is of a more intimate and malleable form than web history or location data.

If a neural device is intended as a neural-controller for a piece of hardware or software, relevant biosignals can be extracted from neural recordings in order to trigger, control and optimise that device or application. However, other information could be derived from the same recordings of those signals by means of subsequent reprocessing and interpreted in ways which present ethical concerns. This is perhaps especially the case given the rate at which recording density is increasing, the greater understanding of how inter-neuron communication affects information processing and the likely increased future role for machine learning in neural data analysis [24].

In terms of the GDPR, individuals whose data is being collected, held or processed are referred to as 'data subjects'. Everyone is at some point a data subject, and may be a data subject in a variety of different ways for different contexts. Given the fact that neural data may be collected, held and processed in various ways, users of neurotechnologies are data subjects in this way. Importantly, especially for regulation as will be discussed in the next section, neural data can be sensitive enough to render a data subject identifiable. Perhaps more importantly from a practical point of view, these signals could be *taken to* identify a data subject, regardless of whether

or not they *actually* do. As such, they could represent a significant issue for a data subject in terms of their otherwise private neural state becoming an apparently open resource from which to characterise them somehow.

We will now take some key concepts from the GDPR and then relate them back to the neural-recording context in order to tease out the implications for consumers and policies.

11.4 The GDPR

Concerns around ethical issues arising from exponential use of brain data such as personality invasion, mental integrity and breach of personhood draw attention to the need to examine legal responses that seek to prevent adverse effects for data subjects [25]. Recital 15 of the GDPR provides neutrality for technology that specifically caters to the protection of natural persons irrespective of the technologies used. This provision aims to reduce the risk of circumvention of the law by recognising potential issues of emerging technologies and their impacts on data protection and seeks to balance the competing interests of privacy and technology [26].

As mentioned above, the GDPR provides data protection measures centred upon persons conceived of as data subjects. One aspect of this includes restrictions and other conditions on the processing of personal data. To assess the role of personal data processing in the context of brain-signal recordings for neurotechnologies, we need to ascertain whether such recordings constitute personal data, and if so, is processing involved.

11.5 Is Brain Data Personal Data?

Personal data in the GDPR is any data that can identify a natural person.

GDPR Art 4 (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Moreover, the European Court of Justice in the case of Breyer vs Germany ruled that the *possibility* of identification is sufficient to consider some data personal data [27]. Readily available neural-recording techniques, like consumer-grade EEG or fMRI, can possibly be used to identify persons [28–31]. Examining the recordings from individuals' brains and using various signal-processing techniques can identify subjects with high accuracy in certain circumstances. It is not implausible to think that these techniques will improve. This ought to prompt discussion over brain reading and mental privacy [32].

Further questions might be raised as to whether certain types of neural recordings might be considered medical data, over and above personal data. According to GDPR Art 4 (15),

… 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

It is certainly the case that neural recordings can serve to indicate diseases such as epilepsy [33]. They can also indicate affective states, including traumatic memory [34]. This permits the possibility of identifying data subjects and their physical or mental health. For now, this analysis will not stray too far into the question of medical data, but will instead just note that it serves to illustrate how one recording may have implications wider than the purposes it is ultimately made for. Neural signals do not need to be recorded for the purpose of identifying data subjects or for identifying physical or mental disease. That information may nonetheless be derived at some stage, through subsequent processing, or through association with other data from other sources, perhaps. The nature of processing neural recordings is of central importance for this reason.

11.6 Is Personal Data Processed in Neurotechnological Devices?

Using the information mentioned, it seems likely that neural recordings in themselves or in combination with other factors are personal data in terms of the GDPR, which brings us to the question of how these personal data are processed. According to GDPR Art 4 (2), it seems clear that neurotechnological devices or systems that use brain-signal recordings also process personal data. In this context, 'processing'

…means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Almost any use of the data, even storage, will be considered 'processing'; collecting it in the first place, assessing it, storing it, sharing it, analysing it, technologically processing it. The key is therefore identifying the data subject and the possibility of linking that data to the subject. If brain data is personal data, and it is processed in particular ways in neurotechnological systems, then it may be characterised as biometric data under the GDPR.

GDPR Art 4 (14) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

As has been referenced already, even EEG recordings can be used to identify subjects. But more to the point, various data that is prohibited by GDPR Art 9 may be processed. This article prohibits the processing of

…biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Neural recordings can be used to predict age [35]. Sex and age can also be predicted where recordings are made for reasons other than making that prediction, in sleep research for instance [36]. Brain recordings have been used to investigate differences among different genders and sexualities, such as the neural difference between homosexual men and heterosexual men and women [37]. Even though these predictions were revealed to be inaccurate in specific cases, the ethical issues arising from the identifiability of persons on that basis remain. A *mis*identification can be just as problematic as an accurate identification, especially where sensitive personal characteristics are involved.

Organisational or social measures can be used to minimise the risks for data subjects in contexts of complex data collection and use. By adding additional layers between collection, retention, processing and the retrieval of data, the chances of misuse or accidental leaks can be minimised. For example, let's imagine Company *A* stores its customers' personal data. The personal data is sent to service provider *B* where a lookup table is created and the data are anonymised. The data are then sent to service provider *C* and put to use in some application (e.g. product functionality, debugging). Service provider *C* will not have access (or rights) to the lookup table held at *B*. Service provider *B* will have a very high level of security and anonymous data-handling expertise. A setup such as this is what can appear in contexts of medical patient data research.

There are risks to this approach, as well. For instance, a data breach at service provider *B* would allow *C* to identify the data subjects. In terms of the European Commission sourced advice for compliance with GDPR, from the advice of Working Party 29,[4] the table held at *B* would need to be deleted (possibly also the underlying data) for the data to be considered properly anonymous. However, especially in the context of medical research, that raises ethical issues regarding incidental findings and, perhaps, the validity of the research, not least in terms of reproducibility.

Perhaps more directly relevant to the context of consumer BCIs using neural recordings, rather than by way of analogy as in medical research and patient data, is the idea of purpose specification. For most data-processing activities, a specific purpose must be set out prior to the use of that personal data. For example, if a company wishes to process my data for the purpose of delivering a service (e.g. updating some software I have purchased from them), they cannot automatically re-use my information for marketing purposes. In scientific research, there is scope for such further use—repurposing of the data—owing to the nature of scientific research as being open-ended.

In scientific research, the scientist(s) may not know how the research will end at the onset (see GDPR Recital 33 and Article 89). But in terms of consumers'

---

[4]This was a working party set up to provide advice while the GDPR was being developed. Its work can be seen at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm [accessed March 2019].

personal data this is not so clear. We need to expand on the recording of brain signals in order to follow up on the potential for repurposing data and how it may raise conceptual and ethical issues relating to consent.

11.7   Recording Brain Signals and the GDPR

In terms of consenting to having brain signals recorded in the first place, questions arise about consenting to potentially unknown outcomes. The question here amounts to how a *specific consent* can be made into a *general collection* with a *wide scope* for repurposing. The stakes are high in terms of the nature of the data as personal or biometric.

Let's imagine a specific scenario where a consumer agrees to the terms of use for a neuro-controlled robotic arm:

Ada likes technology and eagerly purchases the robotic arm. It is controlled via an EEG type cap, with a few electrodes. These electrodes are positioned on the cap with the stated aim of recording brain signals associated with motor cortex activity. Through some training, Ada will be able to control the robotic arm by imagining moving her own limbs. These imagined movements will realise neural activity that the software for her device will come to recognise as control commands for the robotic arm.

It seems clear that Ada agrees to the use of her neural recordings as a control parameter for the robotic arm. The possibility of identifying persons from simple EEG recordings has been alluded to above, so already we see this, at least implicitly, as an agreement to the use of personal data for this purpose. Specifically, she has agreed to motor activity being recorded—that is how the device is stated to work. It is worth noting that some suggest that systems like these are more likely to use facial muscle activity rather than neural activity [38]. But at any rate, the brain is increasingly understood as an open system with distributed functionality. Given the nature of EEG recordings as scalp-based, identifying specific brain areas and specific signals is not simple. Recording brain signals at this level is quite general. Simply due to the physical fact of the EEG cap's distance from the sites of motor neural activity and the impedance of the brain and skull themselves, this may be insufficient to limit the recordings made to purely motor signals.

Recordings of brain signals can be processed in order to create information about specific neural activity, which can be used to infer behavioural, dispositional or other personal data. The scope of the original brain recordings' interpretation is therefore of central importance. The nature of a brain-signal recording as a source of information is open to modification given differing techniques used for processing. It is clear that *existing* signals can be transformed so as to reveal more, or different, information than what they represented at the time of recording. This is what was meant above by distinguishing among specific consent, general collection and a wide scope for repurposing. This makes the processing of data particularly salient.

The nature of data retention, storage and destruction is most pertinent in the case of processing. If 'raw' recordings from Ada's device are retained, they are apt to be reprocessed in ways that were not necessarily consented to. This could amount to a serious repurposing of data, especially in the light of the GDPR. The data might be

processed so as to become biometric data, as per Art 4 (14) mentioned above. These could be used to identify Ada or to infer things about her physical and mental state, her age, gender, sexual orientation and so on. This may be done well or poorly. Furthermore, where AI is involved, the possible scope for repurposing data may not be understood or anticipated fully ahead of time. With this, the issues here are parallel to the ethical issues attending Big Data in general.

Data in general is being collected from a wide variety of devices, in a range of contexts, at an incredible rate (e.g. sensors, internet use, mobile phones). Because of its nature it can't be said to be 'stored' in any conventional sense of the term. For one thing, it is dynamic and it is constantly being updated. It is for these reasons that it is not conventionally accessible, and so is not available without some amount of processing. Big Data provides seemingly endless possibilities for predicting, refining and reconceptualising various domains. These include how financial markets operate, the analysis of social realities and how research is carried out [39]. Beyond data mining [40], Big Data offers a dynamic and huge resource that makes big promises for its users, but which raise ethical concerns [41].

Especially in terms of personal and health data, issues arise concerning the ownership, monetisation and privacy of data. The type of processing that Big Data undergoes, which is necessary to access any of its promised insights, is algorithmic. It is not necessarily related to any particular dataset, but may be a set of sets or a set of sub-sets. The kinds of patterns recognised in data points by algorithms do not preclude the crossing of boundaries among data points. This is the point of algorithmic processing in one sense, as it 'sees' patterns in huge amounts of data that a human would not be able to see.

In this context, the connection between brain data and Big Data can be seen. Big Data can be deployed to answer questions that were not asked at the time of data collection. This does not make data a set of information specific to a research question and a methodology, as might conventionally be the case. Instead, a 'discovery science' attitude can be adopted by researchers in terms of the data itself. It can also lead to a sense in which researchers expect the data to answer questions that have not been thought of yet, leading to a data-driven approach replacing a knowledge-driven one [42, 43]. This leads some in health research to

> …hope we do not fall into the trap of believing that any new information technology is worth using in health research regardless of the ethical issues in performing the research or the larger implications. [44]

AI operating on existing data can, perhaps unpredictably, produce new information or predictions. However, the nature of a neurotechnology system may require that past data be used. Even if this is done only for debugging or optimising the system as a whole, it represents a secondary use of data and may have problematic dimensions if data is re-purposed or identifies specific data subjects.

Systems may require data in order to function optimally. In other words, data collected at one time for a specific purpose may be grouped with other data and processed in order to provide diagnostic data for the system overall. In the context of consumer devices, individuals' recordings may serve to optimise a system-as-product in a general sense. Ada's robotic arm may be one of a million units sold. Each new firmware update may rely on the use of each user's data being processed

in some very general sense. The status of the user's data in such a context is open to question: Is it research data? It seems it can't be anonymous, in any full-blooded sense, as a neural-controlled system adapts to the user as much as they are trained to use that system [45].

At least at some level, the kind of optimisation data, containing lots of processed data from lots of users, must be fed back specifically for each user. This would be how the general processing would lead to specific device optimisation. We must then ask, in the light of the GDPR: How is this curated? The data subject must be identifiable for the optimisation feedback, but the optimisation process of the grouped data seems to rely upon personal data being generally processed. How do we get the flour back from the dough once the loaf is baked? How could it be destroyed, in case Ada grows wary of all this and does not want it anymore? In terms of the GDPR, this amounts to a question about the implementation of the so-called 'right to be forgotten'. When a system-as-product relies on a confluence of multiple users' data collected over time, this seems (at least) very difficult. Central to these questions is the role of consent. With such varying, wide-ranging and apparently open possibilities for the eventual fate of data derived from neural recordings, the possibility of consenting to those recordings is complex.

11.8 Consent

Current data protection regulation strongly emphasises consent. Consent is one of the six legal bases for processing personal data under Article 6 (1) of the GDPR. Processing personal data is generally prohibited, unless the data subject has consented to it or if it is expressly allowed by law.

> GDPR Art 4 (11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;[5]

Specific information must be provided to data subjects where personal data are collected under Article 13(2), including the right to withdraw consent and information regarding automated decision-making or profiling. The GDPR is an improvement from earlier data privacy regimes in that it further promotes and protects the interests of data subjects, including matters of consent, portability and erasure. Current data protection regulation has a strong campaign in favour of consent. As such, wherever data appear, it ought in principle to be identifiable as related to a data subject and, to some degree, be under their control. For instance, if a company holds data on a data subject, that subject ought to be able to get a full rundown of the data held, to rectify inaccurate personal data or insist upon its destruction.

---

[5] Basic requirements for consent are provided in Article 7 and further specified in Recital 32 of the GDPR.

BCIs, in principle, prompt specific issues regarding consent due to their focus on neural signals and the functions of the brain, and thus could have very intimate links to concepts of the self [46]. Given that some users of BCIs may be ill, specific considerations are needed in terms of the major decision-making they may be implicated in. Users of speech prostheses, for example, would require careful attention where end-of-life planning was at stake [47]. But even before these kinds of considerations become relevant, there is the question of the data's collection, storage and processing. These data-specific questions raise consent issues of their own, requiring practicable solutions [48].

Neural devices operate through the extraction of brain signals from neural data that may be produced involuntarily, difficult to individuate because of the recording technique involved and perhaps processed by AI. Depending on what kind of signal is required, different data may be extracted from one set of neural recordings. As has been suggested already, recording brain signals is general while processing brain signals is purpose-relative.

Consent represents an essential factor in how we might conceptualise data issues that may attend neurotechnologies in the near future. It is just one dimension of this conceptualisation, however, in a field growing in complexity, reach and import. How data, once collected, might be reprocessed later has been the focus throughout this chapter, and this hinges on consent. Broad consent, modelled on a bio-banking approach, may be too passive or too reliant on expert decision-making on behalf of data subjects [49]. Dynamic consent, however, relying on technologies to permit user changes to data use may be onerous [50]. Moreover, these may represent other issues in that data would have to be used and re-used in the very process of consent. This could be another issue of the GDPR in terms of data encryption, minimisation and destruction, for instance.

Given the scope for possible uses of brain data and its reprocessing and repurposing, one fear might be that consent itself comes to be seen as an impediment to innovation for this technology. This fear, in which consent comes to be seen as a problem rather than a safeguard, is already discussed in the context of Big Data [51]. Consent, at one very general level, is a means of recognising the autonomy of individuals with all the protections such recognition brings with it, such as non-domination, non-coercion and respect. Challenges to this ought not to be taken lightly. Neurotechnology developers and consumers in general ought to learn from the context of Big Data and avoid this unfortunate outcome.

Specific types of consent, such as those modelled on 'broad consent' as seen in bio-banking contexts, or a technology-driven dynamic consent approach, ought to be bolstered by an effort to encourage a general understanding of neurotechnologies. A better understanding of how neural-based devices work will allow informed decision-making on potential future implications for consenting to brain data collection. This suggests that no particular regime of consent will solve all possible issues arising. A culture of understanding must accompany any solution in order to establish informed attitudes towards technology. Developers of technologies ought to resist overstating or mis-stating the possibilities of their devices in order not to allow a sense of mystery to overcome clarity. This might prevent clear decisions on practical problems regarding data use that would otherwise present themselves.

11.9   Conclusion

It seems that, on the present reading of the GDPR, brain-reading devices present non-trivial consent issues for consumers and developers of the technology. At a conceptual level, they appear to offer only a very complex and convoluted possibility for consenting to their use. This, combined with the likely nature of the way in which the systems will work, makes them a potential challenge for current European data protection standards. Ethically, this is a problem for consumers and developers. This ethical problem could become a legal one if the user of a neurotechnological device were to find themselves unable to exercise their rights owing to the nature of the product they are using.

This has not been a legal analysis, but rather an analysis of the principle of consent and the idea of compliance with the GDPR. There appear to be difficulties, especially where AI processing is involved, in reconciling these factors for neurotechnological devices. This means that better consumer understanding of the stakes must be forthcoming, and that a general awareness of these issues ought to be given from the outset when designing a neuro-controlled device.

References

1. European Commission (2016) 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) (text with EEA relevance).
2. Young BM, Nigogosyan Z, Nair VA, et al. Case report: post-stroke interventional BCI rehabilitation in an individual with preexisting sensorineural disability. Front Neuroeng. 2014;7:18. https://doi.org/10.3389/fneng.2014.00018.
3. Sitaram R, Ros T, Stoeckel L, et al. Closed-loop brain training: the science of neurofeedback. Nat Rev Neurosci. 2017;18:86–100.
4. Roelfsema PR, Denys D, Klink PC. Mind reading and writing: the future of neurotechnology. Trends Cogn Sci. 2018;22:598.
5. Nuffield Council on Bioethics, editor. Novel neurotechnologies: intervening in the brain. London: Nuffield Council on Bioethics; 2013.
6. Pan P, Tan G, Wai P, Aung A. Evaluation of consumer-grade EEG headsets for BCI drone control. In: International researcher club conference on science, engineering and technology, 2017. p. 10–1.
7. Kapur A, Kapur S, Maes P. AlterEgo: a personalized wearable silent speech interface. In: 23rd international conference on intelligent user interfaces. ACM; 2018. p. 43–53.
8. Forrest C. Facebook planning brain-to-text interface so you can type with your thoughts. In: TechRepublic; 2017. https://www.techrepublic.com/article/facebook-planning-brain-to-text-interface-so-you-can-type-with-your-thoughts/. Accessed 14 Nov 2018.
9. Whyte C. Mind-reading headset lets you Google just with your thoughts. New Scientist. 2018.
10. Revell T. Mind-reading devices can now access your thoughts and dreams using AI. New Scientist. 2018.
11. Ings S. Pierre Huyghe at the serpentine—digital canvases and mind-reading machines. Financial Times. 2018.
12. Akst J. Decoding dreams. The Scientist Magazine. 2013.
13. Milne GR, Rohm AJ, Bahl S. Consumers' protection of online privacy and identity. J Consum Aff. 2004;38:217–32.

14. Boyd D, Hargittai E. Facebook privacy settings: who cares? First Monday. 2010. https://doi.org/10.5210/fm.v15i8.3086.

15. Cadwalladr C, Graham-Harrison E. The Cambridge analytica files. The Guardian. 2018. p. 6–7.

16. Howard PN, Kollanyi B. Bots, #Strongerin, and #Brexit: computational propaganda during the UK-EU referendum. Rochester: Social Science Research Network; 2016.

17. Del Vicario M, Zollo F, Caldarelli G, Scala A, Quattrociocchi W. Mapping social dynamics on Facebook: the Brexit debate. Soc Networks. 2017;50:6–16.

18. Teens, Social Media & Technology 2018 | Pew Research Center; 2018.

19. Lankton N, McKnight D, Tripp J. Understanding Facebook privacy behaviors: an integrated model. Faculty Research Day. 2018.

20. Tsay-Vogel M, Shanahan J, Signorielli N. Social media cultivating perceptions of privacy: a 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. New Media Soc. 2018;20:141–61.

21. Collins D, Efford C, Elliot J, et al. Disinformation and 'fake news'. London: The Digital, Culture, Media and Sport Committee; 2019. p. 111.

22. Wong JC. Facebook acknowledges concerns over Cambridge Analytica emerged earlier than reported. The Guardian. 2019.

23. Linus R. What every browser knows about you. In: Webkay; 2019. http://webkay.robinlinus.com/. Accessed 25 Mar 2019.

24. Stevenson IH, Kording KP. How advances in neural recording affect data analysis. Nat Neurosci. 2011;14:139–42.

25. Nijboer F, Clausen J, Allison BZ, Haselager P. The Asilomar survey: stakeholders' opinions on ethical issues related to brain-computer interfacing. Neuroethics. 2013;6:541–78.

26. European Commission. The GDPR: new opportunities. Brussels: New Obligations; 2018.

27. Borgesius FZ. The Breyer case of the court of justice of the European Union: IP addresses and the personal data definition. Eur Data Prot L Rev. 2017;3:130.

28. Bashar K. ECG and EEG based multimodal biometrics for human identification. In: 2018 IEEE international conference on systems, man, and cybernetics (SMC); 2018. p. 4345–50.

29. Abdullah MK, Subari KS, Loong JLC, Ahmad NN. Analysis of the EEG signal for a practical biometric system. World Acad Sci Eng Technol. 2010;4:5.

30. Gui Q, Jin Z, Xu W. Exploring EEG-based biometrics for user identification and authentication. In: Proceedings of the IEEE signal processing in medicine and biology (SPMB); 2014. p. 1–6.

31. Horien C, Shen X, Scheinost D, Constable RT. The individual functional connectome is unique and stable over months to years. NeuroImage. 2019;189:676. https://doi.org/10.1016/j.neuroimage.2019.02.002.

32. Mecacci G, Haselager P. Identifying criteria for the evaluation of the implications of brain reading for mental privacy. Sci Eng Ethics. 2019;25(2):443–61.

33. Staba RJ, Stead M, Worrell GA. Electrophysiological biomarkers of epilepsy. Neurotherapeutics. 2014;11:334–46.

34. Steinert S, Friedrich O. Wired emotions: ethical issues of affective brain–computer interfaces. Sci Eng Ethics. 2019;26:351. https://doi.org/10.1007/s11948-019-00087-2.

35. Al Zoubi O, Ki Wong C, Kuplicki RT, Yeh H, Mayeli A, Refai H, Paulus M, Bodurka J. Predicting age from brain EEG signals—a machine learning approach. Front Aging Neurosci. 2018;10:184. https://doi.org/10.3389/fnagi.2018.00184.

36. Carrier J, Land S, Buysse DJ, Kupfer DJ, Monk TH. The effects of age and gender on sleep EEG power spectral density in the middle years of life (ages 20–60 years old). Psychophysiology. 2001;38:232–42.

37. Alexander JE, Sufka KJ. Cerebral lateralization in homosexual males: a preliminary EEG investigation. Int J Psychophysiol. 1993;15:269–74.

38. Wexler A, Thibault R. Mind-reading or misleading? Assessing direct-to-consumer electroencephalography (EEG) devices marketed for wellness and their ethical and regulatory implications. J Cogn Enhanc. 2018;3:131. https://doi.org/10.1007/s41465-018-0091-2.

39. Mittelstadt BD, Floridi L. The ethics of big data: current and foreseeable issues in biomedical contexts. Sci Eng Ethics. 2016;22:303–41.
40. Fan W, Bifet A. Mining big data: current status, and forecast to the future. SIGKDD Explor Newsl. 2013;14:1–5.
41. Prinsloo P, Slade S. Big data, higher education and learning analytics: beyond justice, towards an ethics of care. In: Daniel BK, editor. Big data and learning analytics in higher education. Berlin: Springer International Publishing; 2017. p. 109–24.
42. Bollier D, Firestone CM. The promise and peril of big data. Washington, DC: Aspen Institute, Communications and Society Program; 2010.
43. Boyd D, Crawford K. Critical questions for big data. Inf Commun Soc. 2012;15:662–79.
44. Rothstein MA. Ethical issues in big data health research: currents in contemporary bioethics. J Law Med Ethics. 2015;43:425–9.
45. Vaughan TM, Heetderks WJ, Trejo LJ, Rymer WZ, Weinrich M, Moore MM, Kübler A, Dobkin BH, Birbaumer N, Donchin E. Brain-computer interface technology: a review of the second international meeting; 2003.
46. Klein E, Ojemann J. Informed consent in implantable BCI research: identification of research risks and recommendations for development of best practices. J Neural Eng. 2016;13:043001.
47. Glannon W. Brain-computer interfaces in end-of-life decision-making. Brain Comput Interfaces. 2016;3:133–9.
48. Kim H, Bell E, Kim J, Sitapati A, Ramsdell J, Farcas C, Friedman D, Feupe SF, Ohno-Machado L. iCONCUR: informed consent for clinical data and bio-sample use for research. J Am Med Inform Assoc. 2017;24:380–7.
49. Steinsbekk KS, Kåre Myskja B, Solberg B. Broad consent *versus* dynamic consent in biobank research: is passive participation an ethical problem? Eur J Hum Genet. 2013;21:897–902.
50. Kaye J, Whitley EA, Lund D, Morrison M, Teare H, Melham K. Dynamic consent: a patient interface for twenty-first century research networks. Eur J Hum Genet. 2015;23:141–6.
51. Kaye J. Abandoning informed consent: the case of genetic research in population collections. In: 267412; 2004. https://repository.library.georgetown.edu/handle/10822/503951. Accessed 20 Feb 2017.