Journal of Law and the Biosciences, 1–19
doi:10.1093/jlb/lsaa051
Original Article

Is the European Data Protection Regulation sufficient to deal with emerging data concerns relating to neurotechnology?

Stephen Rainey[1,*], Kevin McGillivray[2], Simi Akintoye[3], Tyr Fothergill[3], Christoph Bublitz[4] and Bernd Stahl[3]

[1]University of Oxford, Oxford, UK
[2]University of Oslo, Oslo, Norway
[3]De Montfort University, Leicester, UK
[4]University of Hamburg, Hamburg, Germany
*Corresponding author. E-mail: stephen.rainey@philosophy.ox.ac.uk

ABSTRACT

Research-driven technology development in the fields of the neurosciences presents interesting and potentially complicated issues around data in general and brain data specifically. The data produced from brain recordings are unlike names and addresses in that it may result from the processing of largely involuntarily brain activity, it can be processed and reprocessed for different aims, and it is highly sensitive. Consenting for brain recordings of a specific type, or for a specific purpose, is complicated by these factors. Brain data collection, retention, processing, storage, and destruction are each of high ethical importance. This leads us to ask: Is the present European Data Protection Regulation sufficient to deal with emerging data concerns relating to neurotechnology? This is pressing especially in a context of rapid advancement in the fields of brain computer interfaces (BCIs), where devices that can function via recorded brain signals are expanding from research labs, through medical treatments, and beyond into consumer markets for recreational uses. One notion we develop herein is that there may be no trivial data collection when it comes to brain recording, especially where algorithmic processing is involved. This article provides analysis and discussion of some specific data protection questions related to neurotechnology, especially BCIs. In particular, whether and how brain data used in BCI-driven applications might count as personal data in a way relevant to

data protection regulations. It also investigates how the nature of BCI data, as it appears in various applications, may require different interpretations of data protection concepts. Importantly, we consider brain recordings to raise questions about data sensitivity, regardless of the purpose for which they were recorded. This has data protection implications.

KEYWORDS: BCIs, brain data, data governance, GDPR, brain recording, neurotechnology

I. INTRODUCTION

A variety of neurotechnologies are currently available that have functions including monitoring, modulating, stimulating, and imaging activity in brain.[1] Specific types of neurotechnologies can provide novel ways to interact with the world at large. Brain signals interfacing with hardware or software directly require no intervention of the human body upon objects in the world. No physical movement is required in cases of neurotechnology-mediated action, only the realization of a pattern of brain activity.[2]

In principle, the activity of any brain area can be recorded. As cognitive activity is realized by brain activity (or constituted, or subserved by, or correlated with—we remain agnostic on the phrasing), this appears to mean that brain activity corresponding to any cognitive activity is in principle apt to be recorded. This might include specific instances of cognitive activity, forming motor intentions, perceiving across various modalities, reinstating memories, decision-making, and so on.[3] While recording brain activity is a fairly straightforward practice by now, especially using electroencephalography (EEG), the recording of activity is only the first part of a longer chain of processes to arrive at predictions about such activity.

In order to operationalize brain recordings, signals relevant to a given purpose must be extracted from the general recording. For instance, where motor data are required for some application like control of an external robotic limb, motor data must be extracted from the generally recorded signals.[4] This means that in order to make brain recordings useful for a purpose, they must be processed, features extracted, and relevant signals classified according to known features of a particular brain activity. Other processing requires that the recorded signal from an area that is associated with required data is

1 Brendan Z. Allison, Elizabeth Winter Wolpaw & Jonathan R. Wolpaw, *Brain–Computer Interface Systems: Progress and Prospects*, 4 Expert Review of Medical Devices 463–474 (2007).

2 Gerwin Schalk et al., *BCI2000: A General-Purpose Brain-Computer Interface (BCI) System*, 51 IEEE Transactions on Biomedical Engineering 1034–1043 (2004); Jonathan R. Wolpaw et al., *Brain-Computer Interface Technology: A Review of the First International Meeting*, 8 IEEE Transactions on Rehabilitation Engineering 164–173 (2000); Jonathan R. Wolpaw et al., *Brain–Computer Interfaces for Communication and Control*, 113 Clinical Neurophysiology 767–791 (2002), http://www.sciencedirect.com/science/article/pii/S1388245702000573.

3 Shana A. Hall et al., *The Neural Basis of Involuntary Episodic Memories*, 26 Journal of Cognitive Neuroscience 2385–2399 (2014), https://doi.org/10.1162/jocn_a_00633 (last visited Apr. 29, 2019); Ueli Rutishauser, Adam N. Mamelak & Ralph Adolphs, *The Primate Amygdala in Social Perception—Insights from Electrophysiological Recordings and Stimulation*, 38 Trends in Neurosciences 295–306 (2015), http://www.sciencedirect.com/science/article/pii/S0166223615000600 (last visited Feb. 1, 2019); Juha Silvanto, Neil Muggleton & Vincent Walsh, *State-Dependency in Brain Stimulation Studies of Perception and Cognition*, 12 Trends in Cognitive Sciences 447–454 (2008), http://www.sciencedirect.com/science/article/pii/S1364661308002362 (last visited Dec. 13, 2018).

4 F. Lotte et al., *A Review of Classification Algorithms for EEG-Based Brain–Computer Interfaces: A 10 Year Update*, 15 J. Neural Eng. 031005 (2018), https://doi.org/10.1088%2F1741-2552%2Faab2f2 (last visited May 17, 2019).

filtered. This aids in feature extraction, followed by classification. Different methods of classification of brain data types can proceed with various levels of supervision and control. This kind of processing is powerful and can adaptively decode brain data in very fine-grained ways.

According to the OECD, personal brain data are ' . . . data relating to the functioning or structure of the human brain of an identified or identifiable individual that includes unique information about their physiology, health, or mental states.'[5] As such, brain data ought to be of central interest, in the context of personal data protection and the GDPR. The processing of brain data can take the form of adaptive, unsupervised processes or a range of other types of methods. In processing, general brain activity recordings have purpose-specific information reconstructed from them. In principle, multiple processing of the same general brain recording for different purposes could yield different information. What's more, adaptive filtering and classifying can evolve from their initial states. This could mean that processing of brain signal recordings could yield more, or other, information than that intended by a researcher or user (Figure 1).

Brain recordings of this sort may be used to predict future user behavior, brain states, and other aspects of activity pertinent to users' identities.[6] On the face of it, this might indicate that data may be used in a way that requires scrutiny from a data protection perspective, not least in terms of privacy. Some already call for international regulation, especially as consumer neurotechnology enters the market more widely.[7]

We wish to look at the regulation of brain data in terms of the European General Data Protection Regulation (GDPR) which we take as our paradigmatic case of data protection legislation.[8] We will suggest a modified understanding of classifying brain data, and of its sensitivity, to provide better protection of such data.

In order to approach these and related issues, this paper centers on three main areas of enquiry:

1. Whether brain data are personal or health data in the context of GDPR
2. What 'data processing' means, with regard to the GDPR's provisions, in the context of brain data
3. What remaining gaps there may be, where brain data and GDPR are considered (eg such as those related to privacy and security)

This will require discussion of the GDPR itself, as well as the context of emerging neurotechnology. In exploring these areas, we will come to a position on whether the

5 OECD, *Recommendation of the Council on Responsible Innovation in Neurotechnology* (2020), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0457 (last visited Mar. 25, 2020).

6 Philipp Kellmeyer, *Big Brain Data: On the Responsible Use of Brain Data from Clinical and Consumer-Directed Neurotechnological Devices*, Neuroethics. 1–16 (2018), https://doi.org/10.1007/s12152-018-9371-x (last visited May 23, 2019)

7 Marcello Ienca, Pim Haselager & Ezekiel J. Emanuel, *Brain leaks and consumer neurotechnology*, 36 Nat. Biotechnol. 805–810 (2018); Kellmeyer, *supra* note 1

8 Owing to the scope of the authors' research as occurring primarily within Europe, as well as the world-leading ambitions of the GDPR, we limit ourselves for the present discussion to data protection regulation in terms of the GDPR. In terms of the relations between data issues and data protection regardless of jurisdiction, there ought to be various takeaways from our analysis that can be informative for brain data and data protection approaches more broadly.

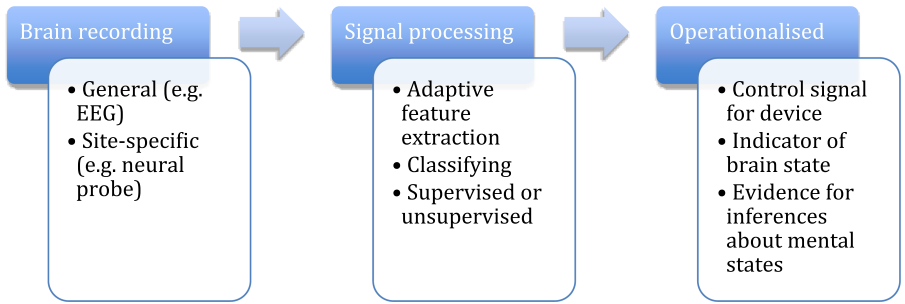

Figure 1. A slice of the generic process from recording of brain signal, via processing, to operationalized signal, omitting feedback loops. The placing of electrodes for the purposes of recording is one way in which specific brain data types can be sought. Filtering of recorded signals according to standard or adaptive algorithms and further classification of what's recorded. In combination, highly specific brain data can be isolated within recorded signals. From these data, information relevant to some purpose can be used as a control feature for a device, or part of a different type of system, such as brain monitoring or medical diagnostics.

present European Data Protection Regulation is sufficient to deal with emerging data concerns relating to neurotechnology.

II. THE EUROPEAN GENERAL DATA PROTECTION REGULATION

First of all, it will be helpful to determine the object of GDPR protections. Among the provisions of the GDPR, individual, natural persons are regarded as 'data subjects,' and it is asserted that each data subject has rights to any and all personal data from which they might be identified. The GDPR is an advance from earlier data privacy regimes in further promoting and protecting the interests of persons *qua* data subjects. This means that companies retaining customer contact details, for instance, must exercise care in sharing, storing, and deleting that data. Different types of data attract different types of protection, depending on sensitivity. Health data sees higher levels of protection than other types, as from this data very sensitive information may be derived about the data subject.

In general, GDPR provisions apply to data subjects in terms of 'the processing of personal data.'[9] In determining whether activities fall within this scope, therefore, two elements must be evaluated. First, the data must be 'processed.'[10] Data protection law takes a much broader view of processing than is generally used by technologists.[11] The processing of personal data includes '...any operation or set of operations which is performed on personal data . . . '[12] Further, the GDPR applies to processing 'wholly or partly by automatic means.'[13] In other words, data processing has a very broad definition and is likely to include most of the operations that are likely to occur in collecting and storing brain data. In terms of this dimension of the regulation, it seems clear that any conceivable BCI will certainly process data in a regulation-relevant way.

The second necessary element for the GDPR to be applicable is that the data must be 'personal.' EU data protection law takes a relatively rigid approach in its application, and determining whether data are personal or not is a crucial element in it.[14] That is, either the law applies completely if the data are determined to be personal data or it falls outside of regulation when it is not.[15] Pursuant to the GDPR, personal data includes:

> . . . *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

9 GDPR Art 4(1).

10 Ibid. Case C-230/14, *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015], [37]. Providing that, the CJEU has held that 'loading personal data on an Internet page must be considered to be "processing" within the meaning of Article 2(b) of Directive 95/46 (judgments in *Lindqvist*, C-101/01, EU:C:2003:596, paragraph 25, and Google Spain and Google, C-131/12, EU:C:2014:317, paragraph 26)'.

11 W. Kuan Hon, Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens (2017).

12 GDPR Art 4(2). *Google Spain SL, Google Inc v Agencia Espannola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez* [2014], [28]. Examples of data processing in the search engine context.

13 GDPR Art 2(1).

14 Hon, *supra* note 33.

15 Although the GDPR recognizes a third citatory of sorts when data are properly pseudonymized, such data are still considered personal, and the GDPR applies. See GDPR Art 4(5).

> 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.[16]

The intention of focusing on personal data is to protect the rights of the data subject. That is, the 'identified or identifiable natural person' to which the data being processed and collected refers.[17] This protection is limited to 'natural' living persons and thus does not include legal or deceased persons.[18] However, the parameters of what constitutes 'personal' data have been debated even before the introduction of the Data Protection Directive.[19] This is unsurprising given the ever-expanding list of technologies capable of collecting data and means with which to profile or link data to individuals.

In determining whether data are personal, the EU data protection law has taken an expansive view.[20] The recent Court of Justice of the European Union (CJEU) case *Nowak v Data Protection Commissioner* provides some context on how broadly the term personal data has been construed.[21] In *Nowak*, a candidate for an accounting certification requested a script after failing the examination.[22] The examination administrative authority and the Irish Data Protection Commissioner determined that an exam script was not personal data and declined to provide the examination script.[23] Consequently, Nowak brought an action before the Irish courts.[24] The main question before the court was whether answers given by a candidate during a professional examination were capable of being personal data.[25] The CJEU determined that written exam answers provided by a candidate could be considered personal data under the broad remit of the Directive.[26]

In its analysis, the CJEU focused on the expansive construction of the 'any information' standard in the Directive, which has been retained in the GDPR, and the correspondingly broad scope regarding the types of data that might qualify as personal data, as long as the information 'relates' to the data subject and allows for a link.[27] Information relates to a data subject when ' . . . by reason of its content, purpose or effect, [it] is linked to a particular person.'[28] The court also emphasized that exam answers were personal to the candidate and were used as the basis of his evaluation.[29] As such,

16 GDPR Art 4(1). Emphasis added.
17 GDPR Art 4(1). See also WP29, 'Opinion 4/2007 on the concept of personal data WP 136' (June 20, 2007) 6.
18 GDPR Art 1(1). GDPR Recital 27.
19 Christopher Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future* (2011), https://www.oecd-ilibrary.org/science-and-technology/regulation-of-transborder-data-flows-under-data-protection-and-privacy-law_5kg0s2fk315f-en (last visited May 23, 2019).
20 WP 29, 'WP 136 Opinion 4/2007 on the concept of personal data' (2007) 4.
21 *Peter Nowak v Data Protection Commissioner* (C-434/16) CJEU [2017].
22 Ibid [18]–[19].
23 Ibid [12]–[14]. The lower Irish courts agreed with the DPC, while the Irish Supreme Court sought a ruling from the CJEU.
24 Ibid [14].
25 Ibid.
26 Ibid [62].
27 Ibid [34].
28 Ibid [35].
29 Ibid [37]–[44].

the candidate had certain rights to the data, including access and rectification.[30] The *Nowak* case signals that like the broad approach to 'processing,' many data types can be considered 'personal.' The ability to identify the data subject, directly or indirectly, or linkability, is central in determining application.[31]

In determining the scope of personal data and measuring or establishing 'linkability,' there has been academic disagreement regarding whether 'objective' or 'relative' criteria should be applied.[32] Oskar Gstrein and Gerard van Eck summarize competing theories for establishing whether data are personal as follows:[33]

> There is an abstract theory (or 'objective criterion') which says that personal data is data that can be tied to a person in view of all the knowledge that exists about it, regardless of the circumstances or the situation or the actors handling it (in legal terms the processor or controller).
>
> The concrete theory (or 'relative criterion') however, focuses on the specific knowledge and means a processor or controller of the data has and only considers data to be personal if an actor is able to tie data to a person in the known circumstances. The difference is that under the abstract theory more data has to be protected and less data is exploitable for economical or other causes.

To determine whether an individual is 'identified or identifiable,' the GDPR sets the boundary at applying 'all the means reasonably likely to be used' to identify the individual.[34] The GDPR definition expands and clarifies that specific identifiers, including those commonly used in digital technologies, may be considered personal or as capable of identifying the data subject.[35] Moreover, by focusing on 'online identifiers' in its definition, the GDPR spells out explicitly that many of the tools used by CSPs can be considered personal data. At Recital 30, the GDPR provides that:

> Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when *combined with unique identifiers and other information received by the servers*, may be used to create profiles of the natural persons and identify them.[36]

Combining Article 4(1) and Recital 30 of the GDPR removes any lingering doubt that technical identifiers may be considered personal data when they provide a link to a

30 Ibid [46].

31 *Peter Nowak v Data Protection Commissioner* (C-434/16) CJEU [2017], [61]–[63].

32 *Breyer v Germany* (C-582/14) CJEU [2016], [25].

33 Oskar Josef Gstrein & Gerard Jan Ritsema van Eck, *Mobile Devices as Stigmatizing Security Sensors: The GDPR and a Future of Crowdsourced "Broken Windows"* (2018), https://papers.ssrn.com/abstract=3105228 (last visited May 23, 2019).

34 GDPR Recital 26. Indirect sources, such as IP addresses, passwords and user IDs, metadata, and insufficiently anonymized data, are considered personal as the data subject can still be identified, even if some additional effort is required. WP29 'Opinion 136 4/2007 on the concept of personal data' (2007) 1–26, 6. See Bygrave (2014) 131. Arguing that the term 'likely' can be equated to an assessment of 'probability', while 'reasonably' establishes the 'difficulty' in making such a connection.

35 GDPR Art 4(1).

36 GDPR Recital 30. Emphasis added.

natural person.[37] However, a technical identifier that does not allow for identification will not be personal data.

In addition to *Nowak v Data Protection Commissioner*, the CJEU case of *Breyer v Germany* provides further clues on evaluating linkability. In *Breyer* the CJEU considered whether a dynamic IP address constitutes personal data when a service provider has the possibility to obtain the additional information necessary to link the IP address to a data subject.[38] In the case, Breyer accessed several public websites operated by German Federal institutions.[39] To counter cyberattacks and criminal activity, the German Federal institutions kept log files of and information on access and use of the websites, including information regarding IP address.[40] Breyer objected to the storage of his IP address information and brought a complaint against the German Federal institutions seeking an order restraining the courts from 'storing, or arranging for third parties to store' such information.[41]

The CJEU noted that '. . . a dynamic IP address does not constitute information relating to an "identified natural person", since such an address does not directly reveal the identity of the natural person who owns the computer . . . '[42] However, the Court went further to consider whether the possibility of combining information related to a dynamic IP address with additional information 'constitutes a means likely reasonably to be used to identify the data subject.'[43] The Court reasoned that the German Federal institutions did have the means 'which may likely reasonably be used' to identify the data subject with the assistance of regulatory authority and the internet service provider.[44] Thus, the Court determined that under the Directive, dynamic IP addresses are considered personal data when the IP address combined with additional information allows for the identification of an individual.[45]

Although *Breyer v Germany* did not necessarily pick an 'objective' or 'relative' approach to determining when data are personal, the case has wider application than IP addresses and likely broadens the types or categories of data that must be protected. However, the CJEU ruling focused on the *possibility* of identification rather than the *likelihood*. Given the ruling in *Breyer v Germany, Nowak,* and text of the GDPR, one seems bound to conclude such identifiers are personal data.

Very complex cases of personal data processing are presented by emerging consumer neurotechnologies. On the foregoing material, it would seem that only totally anonymized data might count as non-personal, as only anonymous data would preclude identification of data subjects. But, given the sorts of functionality intended for consumer neurotechnologies, anonymization would likely render devices practically useless, in not responding to the specifics of their user's brain data.

If, for instance, a brain recording device is intended to respond to specific brain signals produced by a user in order to control a device, then that device will be calibrated

37 If the said identifiers are not used for identifying users, they are not personal data on a *per se* basis.
38 *Breyer v Germany* (C-582/14) CJEU [2016], [30].
39 Ibid [13].
40 Ibid [14].
41 Ibid [17]. The CJEU provided additional details regarding IP addresses and dynamic IP addresses at [36].
42 Ibid [38].
43 Ibid [44].
44 Ibid [48].
45 Ibid [49].

to that user.[46] Classification, or filtration, algorithms will have to operate in specific ways tailored to a user. In the operation of such calibrated algorithms, the instances of use would stand as linkages between a data set and a specific user. A relevant data controller could use the instance of the algorithm's operation to connect the data set to the data subject.

On any of the grounds just described—objective, relative, or via likely or possible linkage with other data—the user would be identifiable by means of the data derived from the brain recording. Even a passive sort of BCI such as EMOTIV's MN8,[47] designed to monitor brain activity for a 'wellness, safety, and productivity' application, might be seen in analogy with the exam question case from *Nowak*, in the sense that the data are personal to the user and the basis for some kind of evaluation of them (eg *too* tired, *over*stressed).

In Table 1, we provide a cursory analysis of data subject identifiability in terms of the GDPR, which summarizes the position that brain recordings ought to be covered by the provisions of the GDPR. Even where derogations apply, such as those for research, it is nevertheless of importance to know that the data meets the description of personal data. This ought to affect the ways in which that data are treated (eg stored, cataloged, shared, destroyed).

While on the face of it, neurotechnologies deal in recordings of electrical signals from brains, what they produce ought to be considered personal data under the scope of data protection regulation. What remains is a discussion of how significant this data may be, how existing regulations ought to be interpreted, and what further regulation may be required. To explore this, it will be informative to discuss some further examples of neurotechnologies, across different contexts.

III. RESEARCH CLAIMS AND APPLICATIONS

Special categories of data enjoy special protection under the GDPR Article 9 and may only be processed where specific conditions are met. These categories are:

> . . . personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, 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 . . .

Recalling Table 1, above, it appears that brain data ought to be considered highly significant data as it can be used to identify a subject uniquely. Apart from the ways in which data subjects might be identified from a data set derived uniquely from their brain by a specific instance of a calibrated classification algorithm, other means of identification are suggested by ongoing research.

46 Dennis J. McFarland & Jon R. Wolpaw, *Brain–Computer Interface Use is a Skill that User and System Acquire Together*, 16 PLoS Biology e2006719 (2018).

47 Workplace Enterprise Solutions„ EMOTIV, https://www.emotiv.com/workplace-wellness-safety-and-productivity-mn8/ (last visited Mar. 12, 2020).

Table 1. Selected text from the GDPR with pertinent questions and commentary relating it to specific neurotechnology cases, highlighting the regulation's applicability to the field

GDPR wording	Consumer neurotechnology applicability
. . . any information relating to an identified or identifiable natural person ('data subject');	Are natural persons *identifiable* from brain signal recordings? Brain signal recordings relate to natural persons. A variety of systems will require calibration to a user, thereby creating a link between the user and their data.
. . . 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	Would brain recordings in general stand as biometric identifiers? Possibly, so relevant to *Breyer v Germany*. Indirect identification by way of online identifiers (eg IP address). Signal processing in a consumer device would likely, technically, be most feasible using a cloud service. This would relate specific individuals to specific brain recordings. This might be *necessary* for accurate decoding. In this instance, the data stored in the cloud service could be used as a link to BCI data, even if the BCI data on its own were too general to identify a data subject.
. . . or to one or more factors specific to the physical, physiological, genetic,	Where the data stand as a basis for evaluating the data subject somehow, as to their mood, stress level etc., this might be analogous with the findings from *Nowak*. Brain signal recordings are capable of revealing specifics about neurophysical information, physiological condition, and possibly genetic features (eg as biomarkers for disease).
. . . mental, economic, cultural or social identity of that natural person	Brain recordings can, or can be taken to, reveal mental content in different degrees of complexity. From these data on likely dimensions of more layered sociopolitical identity can be inferred.[78]

In clinical and research settings, the use of brain–computer interfaces to afford communication and control of brain or motor prostheses is ongoing.[48] One example of

48 BrainCom: Collaborative research project, Neurorehabilitation„ BrainCom, http://www.braincom-project.eu/ (last visited Feb. 19, 2019); Ujwal Chaudhary, Niels Birbaumer & Ander Ramos-Murguialday, *Brain–Computer Interfaces for Communication and Rehabilitation*, 12 Nature Reviews Neurology 513–525 (2016), http://www.nature.com/doifinder/10.1038/nrneurol.2016.113 (last visited Dec. 12, 2017); D. Farina et al., *The Extraction of Neural Information from the Surface EMG for the Control of Upper-Limb Prostheses: Emerging Avenues and Challenges*, 22 IEEE Transactions on Neural Systems and Rehabilitation Engineering 797–809 (2014); *Id.*; Keng Hoong Wee, Lorenzo Turicc & Rahul Sarpeshkar, *An Articulatory*

a rehabilitative brain recording device is that of a speech neuroprosthesis. This presents an interesting example of the potential identifiability of subjects via the recording of brain data as medical data.

Brain signals associated with speech can be recorded from specific articulatory motor areas in the brain.[49] These areas include the brain correlates of movement in the lips, tongue, jaw, and so on. When an individual speaks, these areas are responsible for movements that permit the correct sounds to be made in order to realize intended speech: raising the tongue, constricting the lips, and so on. When speech is imagined, vividly, but not spoken aloud, the same articulatory motor brain areas are activated to a lesser but detectable degree. This activity corresponds to what sound would have been made, even where no vocalization occurs. Through recording these brain signals, unvoiced speech can be reconstructed and realized synthetically via a speaker. Where someone has an impairment in their articulators or is completely paralyzed, this can be exploited via a speech prosthesis in order to realize sound synthetically that would otherwise be impossible.

In the case of a speech prosthesis, the data itself appears to be simply a set of electrical impulses over time. Given their connection to the articulatory motor cortex, however, once processed they represent the speech of a prosthesis user. In terms of the GDPR, as discussed above, this appears to be personal data from which a user could be identified. It would also likely be sensitive data, as it might constitute health data (pursuant Art. 9.1 GDPR).

From a wider research perspective, possible identifiability of individuals from brain signals is an active area. Meanwhile, other areas of ongoing research may point to features of brain activity that could serve as identifiers of data subjects indirectly. Moreover, such data can serve to ground predictions (whether accurate or not) about data subjects' dispositions that include special categories—eg political opinions, biometric data, uniquely identifying data, and sexual orientation. This raises a question as to whether it ought to be considered sensitive data.

A great deal of our cognitive activity is made possible by way of processes that are largely unconscious. From the activation of these automatic processes can be inferred types of cognitive activity or disposition, ranging from basic states of attention or vigilance to moods, emotions, or even complex processes such as reinstating of memory or depression.[50] Dream decoding is another such interesting area of ongoing research,

Speech-Prosthesis System, *in* 2010 International Conference on Body Sensor Networks 133–138 (2010), http://ieeexplore.ieee.org/document/5504741/ (last visited Mar. 19, 2019).

49 Florent Bocquelet et al., *Key considerations in designing a speech brain-computer interface*, 110 Journal of Physiology-Paris 392–401 (2016), http://linkinghub.elsevier.com/retrieve/pii/S0928425717300426 (last visited Nov. 1, 2017); Florent Bocquelet et al., *Real-Time Control of an Articulatory-Based Speech Synthesizer for Brain Computer Interfaces*, 12 PLOS Computational Biology e1005119 (2016), http://journals.plos.org/ploscompbiol/article?id=10.1371/journal.pcbi.1005119 (last visited Apr. 17, 2018).

50 Daniel V. Meegan, *Neuroimaging Techniques for Memory Detection: Scientific, Ethical, and Legal Issues*, 8 The American Journal of Bioethics 9–20 (2008), http://www.tandfonline.com/doi/abs/10.1080/15265160701842007 (last visited Oct. 16, 2018); Sebastian Olbrich & Martijn Arns, *EEG biomarkers in major depressive disorder: Discriminative power and prediction of treatment response*, 25 International Review of Psychiatry 604–618 (2013), https://doi.org/10.3109/09540261.2013.816269 (last visited Aug. 30, 2019).

though in its infancy, wherein AI is coupled with the testimony of those waking from dream states in order to infer visual imagery from dream states.[51]

Research is underway in order to infer personal identity from specific brain activity for use in, for example, biometric security applications.[52] The EEG of BCIs can be deployed as a key part of a biometric authenticator system, based on easily made, low cost, general brain recordings.[53] Studies into this area are small, but if it is the case that brain data obtained via EEG can serve to identify subjects, this is very relevant in light of the GDPR. Further evidence from neuroimaging suggests that the 'functional connectome'—a map of working brain connections throughout the brain—remains stable for periods of time. Finn et al.[54] suggest that '...despite the gross similarities, there is reason to believe that a substantial portion of the brain connectome is unique to each individual.' Identifiability of individuals from brain recordings appears to be possible in this dimension too.

Age, gender, and sexual orientation can be predicted from brain activity.[55] The prediction of political leaning from brain recordings is part of ongoing research as well, with some researchers holding brain activity and structural variation to correlate with political conservatism vs liberalism.[56] Each of these appears to have the potential for high significance in being intended to reveal intimate aspects of a person, some of which fall in the special categories of sensitive data.

Perhaps more importantly from an ethical point of view, brain data could be *taken to* identify sensitive dimensions of a data subject's thoughts and intentions, whether or not they *actually do*. As such, they could represent a significant issue for a data subject in terms of their otherwise private brain states becoming an apparently open resource from which to characterize their thinking processes somehow. This would suggest the high significance of brain data even where its actual usefulness might be overstated. However, how these brain recordings and the data derived therefrom ought

51 T. Horikawa et al., *Neural Decoding of Visual Imagery During Sleep*, 340 Science 639–642 (2013).

52 K. Brigham & B. V. K. V. Kumar, *Subject Identification from Electroencephalogram (EEG) Signals During Imagined Speech*, *in* 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS) 1–8 (2010); Muhammad Kamil Abdullah et al., *Analysis of the EEG Signal for a Practical Biometric System*, 4 World Academy of Science, Engineering and Technology 5 (2010); Qiong Gui, Zhanpeng Jin & Wenyao Xu, *Exploring EEG-based biometrics for user identification and authentication*, *in* In Proc. IEEE Signal Processing in Medicine and Biology (SPMB) 1–6 (2014).

53 Bashar, Chiaki, and Yoshida, *supra* note 15.

54 *Functional Connectome Fingerprinting: Identifying Individuals based on Patterns of Brain Connectivity*, 18 Nat Neurosci 1664–1671 (2015), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5008686/ (last visited May 23, 2019).

55 Sani et al., *supra* note 7; Joel E. Alexander & Kenneth J. Sufka, *Cerebral Lateralization in Homosexual Males: a preliminary EEG investigation*, 15 International Journal of Psychophysiology 269–274 (1993), http://www.sciencedirect.com/science/article/pii/016787609390011D (last visited Jan. 21, 2019); Julie Carrier et al., *The effects of age and gender on sleep EEG power spectral density in the middle years of life (ages 20–60 years old)*, 38 Psychophysiology 232–242 (2001), https://www.cambridge.org/core/journals/psychophysiology/article/effects-of-age-and-gender-on-sleep-eeg-power-spectral-density-in-the-middle-years-of-life-ages-2060-years-old/6EEF6E7C474335483533DA06164A9B26 (last visited Jan. 21, 2019).

56 Ryota Kanai et al., *Political Orientations Are Correlated with Brain Structure in Young Adults*, 21 Curr Biol 677–680 (2011), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3092984/ (last visited Mar. 25, 2020); Kristine M. Knutson et al., *Politics on the brain: An fMRI investigation*, 1 Social Neuroscience 25–40 (2006), https://doi.org/10.1080/17470910600670603 (last visited Mar. 25, 2020).

to be considered is a difficult question. In terms of the GDPR, it is definitely *processed*. In being an identifier of a data subject, either on its own or through linkage with other data, it is also *personal*. In these research applications, it also appears to be highly significant data which could qualify as *sensitive*.

What's more, given the use of adaptive, algorithmic, feature extraction, and classification—or machine learning generally in processing and decoding brain data—we have to bear in mind that further advances in computing may have a bearing on the identifiability of subjects given existing data sets.[57] A data set that now may not identify a subject could become one that does, give some particular advance in machine learning.

This raises the possibility that repurposing of data sets already in existence might yield identifiability of subjects that were not identifiable in the first place, upon collection of the data. This appears similar to the discussion above concerning 'technical identifiers' and *Breyer vs. Germany*. There is the possibility, even if not the likelihood, that brain data collected that in itself appears not to identify a subject may, upon repurposing or in combination with other data, identify a data subject and ground predictions about sensitive dimensions of their identity.

IV. GROWING CONSUMER CONTEXT

Consumer devices can make brain recordings, whether or not they are capable of processing them according to their stated aims[58] or discriminating among the signals recorded in a fine-grained way. These data and their potential reuse by third parties (particularly in legislative contexts which regulate medical devices separately from commercial devices) may pose serious ethical and data protection concerns.

There is a range of non-medical applications devices in development, for applications from gaming to the workplace. Currently marketed devices, eg by Emotiv, Neurosky, are not yet as commonplace as mobile phones, laptop computers, and so on. This might be owing to the absence of apps, or issues with ease of use, or perhaps just a lack of perceived need. However, various popular media reports reveal more tech companies announcing their entrance to the field, investing significant sums. These developments highlight the intention to develop consumer brain–interfaces to link computers with the brain, directly. With the kind of financial backing possible from tech companies, and high profile offered by figures like Elon Musk, such efforts are unlikely to be a flash in the pan.

Kernel, a multimillion-dollar company based in Los Angeles, wants to 'hack the human brain.'[59] More recently, they are joined by Facebook, who wants to develop a means of controlling devices directly with data derived from the brain.[60] Meanwhile,

57 Lotte et al., *supra* note 9.

58 Anna Wexler & Robert Thibault, *Mind-Reading or Misleading? Assessing Direct-to-Consumer Electroencephalography (EEG) Devices Marketed for Wellness and Their Ethical and Regulatory Implications*, 3 J Cogn Enhanc (2018), https://doi.org/10.1007/s41465-018-0091-2 (last visited Oct. 10, 2018).

59 Nick Statt, *Kernel is Trying to Hack the Human Brain—But Neuroscience has a Long Way to Go*, The Verge 131–137 (2017), https://www.theverge.com/2017/2/22/14631122/kernel-neuroscience-bryan-johnson-human-intelligence-ai-startup (last visited May 23, 2019).

60 Conner Forrest, *Facebook Planning Brain-to-Text Interface So You Can Type with Your Thoughts*, TechRepublic (2017), https://www.techrepublic.com/article/facebook-planning-brain-to-text-interface-so-you-can-type-with-your-thoughts/ (last visited Nov. 14, 2018); Olivia Solon, *Facebook has 60 People*

Elon Musk's 'Neuralink' is a venture which aims to 'merge the brain with AI.'[61] This sounds likely to be based in recording and stimulating the brain, though details are far from clear at this point regarding what exactly 'merging' with AI would amount to. Nevertheless, Musk's proposed mode of electrode placement, modeled on a sewing machine, appears interesting in terms of the high-density recording it would enable (though it is not clearly applicable for a human brain-sized target, rather than that of a rat).[62]

A commercial enterprise with sufficient data and signal processing capacity might be well placed to derive potentially sensitive information from an ensemble of recorded brain activity fairly meaningless in itself. This might be exacerbated through the use of adaptive, learning algorithms operating on large amounts of data. A wide variety of user information might be inferred, all without users having anything special to do.[63] All is needed is that they use their computer via the BCI. They may not even be aware of recording. These reactions are also not under the conscious control of the person, so in a sense, they tap into the unconscious. However, we hasten to note that fears about reading out thoughts or the content of mental states are premature.[64]

This idea, which from highly significant brain data sensitive data may be inferred, is of importance in terms of the Article 9.1 of the GDPR. The way data are classified as sensitive or not affects the degree of protection afforded by the regulation, and in the GDPR, this classification is based on recording purpose. If brain data are gained through medical devices, eg BCI in motor or speech rehabilitation, it regularly qualifies as health data. However, if it stems from consumer neurotech and recordings of the type envisioned by Facebook, Kernel, and Neuralink, the data might seem not to constitute health data. It is not recorded for health-related applications, and so apparently is not health data.

Regarding health or medical data (GDPR Article 4 (13–15) defines data types), Article 9 prohibits processing, unless exceptions are met. In summary, if special category data are to be processed, there must be a legal basis under Article 9 in addition to a legal basis under GDPR Article 6.

Special category data are defined in terms of the purposes for which the data are collected. This idea of data definition in terms of recording purpose appears to be inadequate for brain recordings, especially in a consumer context. Brain recording devices can generate a lot of data. From the large amount of data collected, just a subset may be of direct relevance for the operation of the devices they will control.

Working on How to Read Your Mind, The Guardian, April 19, 2017, https://www.theguardian.com/technology/2017/apr/19/facebook-mind-reading-technology-f8 (last visited Nov. 14, 2018).

61 Rolfe Winkler, *Elon Musk Launches Neuralink to Connect Brains With Computers*, Wall Street Journal, March 27, 2017, https://www.wsj.com/articles/elon-musk-launches-neuralink-to-connect-brains-with-computers-1490642652 (last visited May 23, 2019).

62 Elon Musk & Neuralink, *An Integrated Brain-Machine Interface Platform With Thousands of Channels*, 21 Journal of Medical Internet Research e16194 (2019), https://www.jmir.org/2019/10/e16194/ (last visited Mar. 10, 2020).

63 Ali Bashashati et al., *A Survey of Signal Processing Algorithms in Brain–Computer Interfaces Based on Electrical Brain Signals*, 4 J. Neural Eng. R32 (2007), http://stacks.iop.org/1741-2552/4/i=2/a=R03 (last visited Jan. 21, 2019).

64 Pim Haselager & Giulio Mecacci, *Is Brain Reading Mind Reading?*, *in* Neurolaw and Responsibility for Action 182–192 (Bebhinn Donnelly-Lazarov ed., 1 ed. 2018), https://www.cambridge.org/core/product/identifier/9781108553339%23CN-bp-8/type/book_part (last visited Oct. 29, 2018).

The remainder could be thought of as a kind of brain data exhaust. Whereas GDPR provisions may appear highly relevant in terms of the recordings made by various devices, it seems a purpose definition of data sensitivity could mean the data derived from recordings superfluous to the specific purpose could simply bypass regulation.

It seems quite clear that a trove of data exhaust, besides operational material, is something that technology companies will be very interested in using. This will represent a data asset for various activities continuous with the interests they have already. Such interests include the profiling human behavior through datafication, for both engineering and non-engineering reasons.[65] This has also led to experiments in manipulation, based on social media data.[66] This kind of information would be of undeniable value in a variety of possible ways, including but not limited to *neuroprofiling*. There are many ways in which this might be problematic.

From a data protection perspective, this is interesting. Evaluating whether use (and reuse) is compatible with the lawful basis for which the data was collected is a complex undertaking. If data are processed in a manner that is incompatible with the purpose for which it was initially obtained, the processing is unlawful. If data are used for a purpose beyond that for which it was collected, it is considered to have been 'repurposed.'

For example, in the case of a consumer device that collected a lot of data from its users in order to optimize the functioning of the device and its applications, it may not be the case that such processing was *incompatible* with the purposes for which it was obtained. Implicit in the purchase of the device and the software agreement might be the acceptance of measures to optimize the device, which might include subsequent processing of data. But it may be the case that such a use amounted to a repurposing of that data. This kind of distinction would need to be made clear in the terms of use for the device. In general, at the minimum, reprocessing is another form of processing that requires consent from the user of such a device.

Given the possibility of algorithmic processing and the likelihood that algorithms themselves develop beyond their initial states, how a static agreement could account for an open future of possibilities is very unclear. What's more, where the optimization of a device relied upon algorithmically processed, repurposed data, it would be extremely difficult to account for how any given user of a device could seek the removal of their data from such an arrangement.

Brain data might be easily instrumentalized for a variety of purposes, even more in the context of increasing algorithmic sophistication and normalization of Big Data. The events surrounding Cambridge Analytica and Brexit should illustrate well the cause for concern where profiling can serve to occlude the uses of information from the targets

65 Ashish Thusoo et al., *Data Warehousing and Analytics Infrastructure at Facebook*, *in* Proceedings of the 2010 ACM SIGMOD International Conference on Management of Data 1013–1020 (2010), http://doi.acm.org/10.1145/1807167.1807278 (last visited May 23, 2019); Jose van Dijck, *Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology*, 12 1 197–208 (2014), https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/datafication (last visited May 23, 2019).

66 Adam D. I. Kramer, Jamie E. Guillory & Jeffrey T. Hancock, *Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks*, 111 PNAS 8788–8790 (2014), https://www.pnas.org/content/111/24/8788 (last visited May 23, 2019).

of that information use.[67] It seems clear that this is highly significant data, but it is not necessarily definable as sensitive where recording purpose is what classifies data. As such, this represents a gap in regulation and prompts further discussion of other such gaps.

V. GAPS IN POLICY AND SECURITY

Research applications of neurotechnology have various allowances within the text of the GDPR, but these amount only to relaxed versions of the existing protections. Where personal data are present, even in a research context, the GDPR applies. But the exact nature of technologies deriving from primary research is not necessarily very clear. A consumer device, for instance, might be classifiable as a medical device, depending on what it does. Consumer devices often use terms like 'wellness' to avoid much stricter medical product requirements. But functionally, the data the record could well be classifiable as biometric or medical data, especially where repurposed for some reason. Between these and any other classifications of the technology, differences in applicability of data protection rules might emerge.

What's more, depending upon the nature of a device's functioning, variations in data protection applicability may apply. Where brain data are recorded by a device and stored in a cloud service along with brain recordings from other devices, this would have different implications than a device that did not save recordings but processed brain signals locally, in real time, for some application. And again, the nature of the application realized by the device would affect how that device would fit with data protection regulation; is it aimed at recreation? self-monitoring? detecting disease?

The question is whether brain data are adequately accounted for by the categories used in the GDPR. We need to ask whether brain recording cases deserve the kind of strong protection offered to medical or health data, even though they may not at present fit into those categories. We should moreover ask whether the level of protection of medical data is sufficient. Perhaps intimate brain data should enjoy stronger protection.

Given that the data recorded from neurotechnological devices should be considered personal data, especially in combination with other information, the security of this data and related processing operations should be ensured for reasons of compliance with the GDPR and alignment with ethical principles. There is a recognition that violation of this security can result not only in physical harm to users but also that it threatens their autonomy, agency, and sense of authenticity.[68] Continuing discourse on the topic of 'neurorights,' or a reframing of extant human rights combined with

67 Michela Del Vicario et al., *Mapping Social Dynamics on Facebook: The Brexit Debate*, 50 Social Networks 6–16 (2017), http://www.sciencedirect.com/science/article/pii/S0378873316304166 (last visited Mar. 21, 2019); Philip N. Howard & Bence Kollanyi, *Bots, #Strongerin, and #Brexit: Computational Propaganda During the UK-EU Referendum* (2016), https://papers.ssrn.com/abstract=2798311 (last visited Mar. 21, 2019); Julia Carrie Wong, *Facebook Acknowledges Concerns Over Cambridge Analytica Emerged Earlier than Reported*, The Guardian, March 22, 2019, https://www.theguardian.com/uk-news/2019/mar/21/facebook-knew-of-cambridge-analytica-data-misuse-earlier-than-reported-court-filing (last visited Mar. 25, 2019); C. Cadwalladr & E. Graham-Harrison, *The Cambridge Analytica Files*, The Guardian, Mar. 18, 2018, at 6–7, http://davelevy.info/Downloads/cabridgeananalyticafiles%20-theguardian_20180318.pdf (last visited Mar. 21, 2019).

68 Kellmeyer, *supra* note 1.

novel human rights to preserve brain privacy, ought to grow in parallel with developing neurotechnologies.

In practice, however, substantial gaps in privacy and security are evident, from the reported use of a BCI to extract concealed information in 2011 to the concerning results of a security vulnerability test on a widely available headset marketed directly to consumers.[69] Despite the 15-year existence of the term 'neurosecurity,'[70] and calls for attention to the threat of cyberattacks on BCIs,[71] a host of challenges and barriers to secure data storage, processing, and sharing remain. Some of these are technical, eg the inherent vulnerabilities in Bluetooth,[72] which has frequently been used in commercial BCIs, and cloud computing systems,[73] a necessity of high-volume storage.

Progress has been made in terms of addressing some security gaps, including the advancement of practical solutions such as the 'BCI Anonymizer'[74] and privacy-preserving architecture models.[75] However, the applications of such methods are limited; the former would substantially reduce the usability of the data, while the latter only addresses one operational link within the wider processing context. Likewise, suggesting the use of blockchain for brain data would potentially violate EU data subject rights to rectification and erasure under Article 17 of the GDPR.

VI. CONCLUSIONS

We have two main conclusions concerning brain data with respect to current European data protection approaches. These are related to the nature of brain data and the ramifications this ought to have for its classification in the GDPR:

1. Brain data are a special case of data in the sense that its significance can vary depending upon its processing, regardless of the purpose of its capture.
    - Categorization of brain-derived data is unclear in terms of the GDPR when it is not about health, nor stemming from medical devices.
2. Data protection legislation ought to differentiate data sensitivity among data types based on the potentiality that data have for revealing personal data via processing or repurposing, not based in the purposes for which the data are collected.

---

69 J. Peter Rosenfeld, *P300 in Detecting Concealed Information*, Memory Detection: Theory and application of the concealed information test (2011), https://www.scholars.northwestern.edu/en/publications/p300-in-detecting-concealed-information (last visited May 23, 2019).

70 J. R. Millan et al., *Noninvasive Brain-Actuated Control of a Mobile Robot by Human EEG*, 51 IEEE Transactions on Biomedical Engineering 1026–1033 (2004).

71 Tamara Denning, Yoky Matsuoka & Tadayoshi Kohno, *Neurosecurity: Security and Privacy for Neural Devices*, 27 Neurosurg Focus E7 (2009).

72 Brian Cusack, Kaushik Sundararajan & Reza Khaleghparast, *Neurosecurity for Brainware Devices*, in The Proceedings of 15th Australian Information Security Management Conference, 49–56 (C. Valli ed., 2017), https://ro.ecu.edu.au/ism/206.

73 Ienca, Haselager, and Emanuel, *supra* note 5.

74 Tamara Bonaci, Ryan Calo & Howard Jay Chizeck, *App Stores for the Brain: Privacy and Security in Brain-Computer Interfaces*, 34 IEEE Technology and Society Magazine 32–39 (2015).

75 Cho Kwon, Donghyeok Lee & Namje Park, *Design of Secure EEG Collection Model based on Privacy-preserving BCI in Big Data Environment*, 118 International Journal of Applied Mathematics 851–861 (2018).

- Data from BCIs and other brain recordings is often personal and may be as sensitive as health data.

Together, these conclusions point to how brain data can be accommodated within the provisions of the GDPR, as long as they are interpreted and applied appropriately. Practically speaking, brain data should be considered on a par with medical data and be treated as sensitive. Brain data can have consequences as sensitive as the other forms of data in the category of special protection. Its potentiality for identifying persons and for revealing sensitive characteristics through being processed is very high.

This kind of categorization as sensitive data would provide a first layer of security for brain recordings. This is made all the more pressing in a context of increasing algorithmic complexity and effectively unlimited data storage. Big data concerns ought to be reflected where brain recording and algorithms converge, in terms of data subject identifiability as well as data security. With current GDPR provisions, this can be reflected by ascribing to brain recordings the highest protection status—that of medical data.

However, beyond GDPR there are further BCI-related data concerns. It may not be enough to afford appropriate protections for data subjects by means of regulation. As is widely known from the way smartphones are put to use, in terms of common apps and social media especially, data subjects readily consent to having their data recorded and used, if they get something useful in return.[76] We pay with data for goods and services. Very likely, this will be the business model for brain data as well. And for this, the current GDPR—and policy in general—does not offer satisfying solutions to deal with these kinds of social behaviors. Data risks will persist, in this context, with highly sensitive data at stake. The increased data literacy, called for by Kellmeyer,[77] ought to become a focal point for discussion across different levels of societies.

For policymakers, failures in social media data policy ought to inform a lively approach to discourse surrounding neurotechnological data issues. It is not too early for policymakers to anticipate neurotechnology, in policy discourse, as it is a burgeoning field being developed at a fast pace. Delaying discussion may seem prudent in some respects about not stifling innovation, but overall it is advisable to begin as soon as possible to pre-empt future data crises. A pre-emptive approach might also serve to minimize the need to formulate novel legal 'neurorights' in reaction to emerging technology.

---

76 Michael Zimmer, *"But the Data is Already Public": On the Ethics of Research in Facebook*, 12 Ethics Inf Technol 313–325 (2010), https://link.springer.com/article/10.1007/s10676-010-9227-5 (last visited Feb. 22, 2017); Danah Boyd & Eszter Hargittai, *Facebook Privacy Settings: Who Cares?*, 15 First Monday (2010), https://journals.uic.edu/ojs/index.php/fm/article/view/3086 (last visited June 7, 2020).

77 Kellmeyer, *supra* note 143.

78 cf William E. Connolly, Neuropolitics: Thinking, Culture, Speed (2002); Drew Westen et al., *Neural Bases of Motivated Reasoning: An fMRI Study of Emotional Constraints on Partisan Political Judgment in the 2004 US Presidential Election*, 18 Journal of cognitive neuroscience 1947–1958 (2006).

For users of consumer neurotechnologies, it should be paramount that they ought to seek information on *exactly what* a neurotechnology does, regardless of marketing claims. Increased data literacy would be valuable and support the anticipation of future privacy and security issues. But in no way should the onus fall solely on the consumer to increase this data literacy.

Cross-sector, multidisciplinary, and multi-sector dialogs on brain data privacy and security are a pressing necessity due to the increasingly broad nature of neurotechnology development and device use. Responsible data protection practices, incorporating relevant ethical and legal concepts, provide a promising method of addressing issues around brain data and the future implications of neurotechnologies.

VII. FUNDING AND ACKNOWLEDGEMENTS

The authors gratefully acknowledge funding from the BrainCom Project, Horizon 2020 Framework Programme (732032). Christoph Bublitz acknowledges funding through the German Ministry of Education and Research, INTERFACES, 01G1622B. Additionally, this research has received funding from the European Union's Horizon 2020 Framework Programme for Research and Innovation under the Specific Grant Agreement Nos 785907 and 945539 (Human Brain Project SGA2 and SGA3).