Journal of Law and the Biosciences, 1–25
https://doi.org/10.1093/jlb/lsac025
Original Article

Addressing privacy risk in neuroscience data: from data protection to harm prevention

Anita S. Jwa * and Russell A. Poldrack

Department of Psychology, Stanford University, 450 Jane Stanford Way, Building 420, Stanford, CA 94306, USA
*Corresponding author. E-mail: anniejwa@stanford.edu

ABSTRACT

A recent increase in the amount and availability of neuroscience data within and outside of research and clinical contexts will enhance reproducibility of neuroscience research leading to new discoveries on the mechanisms of brain function in healthy and disease states. However, the uniquely sensitive nature of neuroscience data raises critical concerns regarding data privacy. In response to these concerns, various policy and regulatory approaches have been proposed to control access to and disclosure of neuroscience data, but excessive restriction may hamper open science practice in the field. This article argues that it may now be time to expand the scope of regulatory discourse beyond protection of neuroscience data and to begin contemplating how to prevent potential harm. Legal prohibition of harmful use of neuroscience data could provide an ultimate safeguard against privacy risks and would help us chart a path toward protecting data subjects without unduly limiting the benefits of open science practice. Here we take the Genetic Information Non-Discrimination Act (GINA) as a reference for this new legislation and search for answers to the core regulatory questions based on what we have learned from the enactment of the GINA and the merits and weaknesses of the protection it provides.

KEYWORDS: neuroscience, neuroethics, data privacy, Genetic Information Nondiscrimination Act

I. INTRODUCTION

There recently has been a substantial increase in the collection, processing, and sharing of neuroscience data. A number of research initiatives and data repositories were established during the last few decades to facilitate sharing of neuroscience data, and funding agencies have begun to require that investigators share data collected as part of funded research.[1] Advances in methods to monitor and record brain activity have also enabled investigators to obtain a large amount of data from individual subjects' brains. Technological developments in neuroscience combined with artificial intelligence (AI) and big data analytics have accelerated the speed and scale of data processing and analysis. With the aid of these novel software tools and algorithms to analyze massive datasets, neuroscience research has entered into the era of big data.[2] In addition, neuroscience data have become increasingly available outside research and clinical contexts, as academic and healthcare institutions have begun to form partnerships with large tech companies to share data, including neuroscience data. The emergence of direct-to-consumer devices and applications, such as electroencephalogram (EEG), brain–computer interface (BCI), and transcranial electrical stimulation (tES) devices, has also prompted the for-profit collection, use, and sharing of neuroscience data.[3]

The increase in the amount and availability of neuroscience data will enhance the rigor and reproducibility of neuroscience research and potentially enable new discoveries on the mechanisms of brain function in both healthy and disease states. However, at the same time, it also raises critical ethical issues, such as data privacy.[4] Neuroscience data are often combined with personal sensitive information (eg diagnosis of a neurological disorder or genetic composition of data subjects), and the sharing and reprocessing of neuroscience data could potentially cause unwanted disclosure of this sensitive information. Reverse inference from neural recording or neuroimaging data could unveil subjects' cognitive and affective states.[5] Studies have suggested that it may also be possible to predict future outcomes on the basis of neuroscience data—for example, the risk of developing a neurological disorder (eg Alzheimer's disease)[6] or even criminal propensity,[7] which raises concerns regarding premature or discriminatory use of this information against data subjects. Furthermore, deciphering one's cognitive and affective states, not to mention potentially altering these states using neuromodulation technology, could encroach on our most intimate sphere of mental privacy, namely, the brain.[8]

[1] Anita S. Jwa & Russell A. Poldrack, *The Spectrum of Data Sharing Policies in Neuroimaging Data Repositories*, Hum. Brain Mapp. (2022).

[2] Damian O. Eke et al., *International Data Governance for Neuroscience*, 110 Neuron (2022); Suprana Choudhury et al., *Big Data, Open Science and the Brain: Lessons Learned from Genomics*, 8 Front. Hum. Neuroscience (2014).

[3] Iris Coates McCall & Anna Wexler, *Chapter One - Peering into the Mind? The Ethics of Consumer Neuromonitoring Devices*, in Developments in Neuroethics and Bioethics (Imre Bárd & Elisabeth Hildt eds., 2020); Karola V. Kreitmair, *Dimensions of Ethical Direct-to-Consumer Neurotechnologies*, 10 AJOB Neurosci. 152 (2019).

[4] James Eberwine & Jeffery Kahn, *The BRAIN Initiative and Neuroethics: Enabling and Enhancing Neuroscience Advances for Society*, 11 AJOB Neurosci. 135 (2020).

[5] Russell A. Poldrack, *Inferring Mental States from Neuroimaging Data: From Reverse Inference to Large-scale Decoding*, 72 Neuron 692 (2011).

[6] Peter N. E. Young et al., *Imaging Biomarkers in Neurodegeneration: Current and Future Practices*, 12 Alzheimer's Res. Ther. (2020).

[7] Leda Tortora et al., *Neuroprediction and A.I. in Forensic Psychiatry and Criminal Justice: A Neurolaw Perspective*, 11 Front Psychol. (2020); Eyal Aharoni et al., *Neuroprediction of Future Rearrest*, 110 Proc. Natl. Acad. Sci. 6223 (2013).

[8] Marcello Ienca & Roberto Andorno, *Towards New Human Rights in the Age of Neuroscience and Neurotechnology*, 13 Life Sci. Soc. Policy (2017); Rafael Yuste et al., *Four Ethical Priorities for Neurotechnologies and AI*, 551 Nature (2017).

In response to these concerns, various policy and regulatory approaches have been proposed to protect neuroscience data. Most of these approaches have focused on controlling access to and disclosure of neuroscience data, such as requiring more granular consent to data sharing, imposing strict limitations on who can access to data for what purposes, applying rigorous data protections (such as deidentification or encryption of data), or creating novel human rights to protect mental privacy.[9] These approaches would heighten the protection of neuroscience data, but excessive restriction on access to and sharing of the data might hamper open science practice and scientific advancement in neuroscience.

Regulatory action should be an outcome of rigorous balancing of risk to an individual's privacy interest in neuroscience data versus societal benefits of collection and analysis of neuroscience data to further neuroscience research.[10] When assessing the privacy risk associated with neuroscience data, we should consider both the likelihood and the magnitude of harm resulting from potential infringement on privacy. Although the literature on drawing inference from neuroscience data is extensive, currently there is insufficient evidence that neuroscience data can reliably decode complex cognitive and affective states or provide precise predictions of future outcomes.[11] In addition, unwanted or illicit disclosure of neuroscience data alone would rarely inflict harm to a data subject unless a nefarious actor explicitly abuses sensitive information in the data to harm the subject. Moreover, even with rigorous restrictions, achieving complete privacy would not be possible given the exponential growth of available neuroscience data and technical advancements in big data analytics.

In this article, we argue that it may now be time to expand the scope of regulatory discourse beyond protection of neuroscience data and to begin contemplating how to prevent potential harm. Legal prohibition of harmful use of neuroscience data could provide an ultimate safeguard against privacy risks associated with neuroscience data and would help us chart a path toward protecting data subjects without unduly limiting the benefits of open science practice in neuroscience. This article begins with a review of privacy concerns around neuroscience data and examines regulatory and policy proposals in the literature to address these concerns. Then it outlines the need for new legislation against misuse of information inferred from neuroscience data. Finally, some of the core regulatory questions arising from developing this new legislation are discussed within. Here we take the Genetic Information NonDiscrimination Act (GINA), a federal law prohibiting discriminatory use of genetic information, as a reference for this new legislation and search for answers to the core regulatory questions based on what we have learned from the enactment of the GINA and the merits and weaknesses of the protection it provides.

[9] See, eg, Eke et al., *supra* note 2; Sara Goering et al., *Recommendations for Responsible Development and Application of Neurotechnologies*, 14 NEUROETHICS 365 (2021); Marcello Ienca, et al., *Towards a Governance Framework for Brain Data*, 15 NEUROETHICS (2022).

[10] Hester J. Ward, *Privacy and Governance Implications of Wider Societal Uses of Brain Imaging Data*, 47 CORTEX 1263 (2011). DOI: https://doi.org/10.48550/arXiv.2109.11960.

[11] Mahan Hosseini et al., *I Tried a Bunch of Things: The Dangers of Unexpected Overfitting in Classification of Brain Data*, 119 NEUROSCI. BIOBEHAV. REV. 456 (2020); Russell A. Poldrack, Grace Huckins, & Gaël Varoquaux, *Establishment of Best Practices for Evidence for Prediction: A Review*, 77 JAMA PSYCHIATRY 534 (2020); Gaël Varoquaux, *Cross-validation Failure: Small Sample Sizes Lead to Large Error Bars*, 180 NEUROIMAGE 68 (2018).

II. WHAT ARE NEUROSCIENCE DATA, AND WHY ARE THEY SPECIAL?

Neuroscience data, or brain data, have been defined in various ways in the literature. Some presented rather broad views—'data collected from the brains of humans'[12] or 'quantitative data about human brain structure, activity, and function'.[13] However, for the sake of our regulatory analysis, a more specific definition would be desirable because it would allow us to more precisely demarcate what information should be protected. Here we follow the definition of neuroscience data suggested in Eke and colleagues' recent article, that neuroscience data are 'raw measurements of nervous system structure, operational properties, and function' along with derived data and metadata describing the processing steps and analyses used to produce derived data.[14] Raw data on the nervous system can be collected using various modalities that measure the structure (eg magnetic resonance imaging (MRI) and computed tomography (CT)) and the function of the brain (eg direct intracranial electrical recordings, electroencephalogram (EEG), magnetoencephalography (MEG), functional magnetic resonance imaging (fMRI), functional near-infrared spectroscopy (fNIRS), and positron emission tomography (PET)), ranging from single- or multi-unit-level data to system-level or whole-brain-level data.

The open science movement in the field of neuroscience has led to development of a number of data sharing platforms globally. For example, International Neuroimaging Data-Sharing Initiative,[15] OpenNeuro,[16] Human Connectome Project,[17] and the Alzheimer's Disease Neuroimaging Initiative[18] are some of the notable neuroscience data repositories in the USA. Most of these repositories were established and continue to be supported by the US federal funding agencies, such as the National Institutes of Health or the BRAIN Initiative.[19] Repositories in the European Union include EBRAINS,[20] a data sharing infrastructure created by the Human Brain Project, and the UK Biobank,[21] a large-scale biomedical database encompassing various types of data including neuroimaging data. The Canadian Open Neuroscience Platform is another relatively new database intended to facilitate open science within both the basic and clinical neuroscience community.[22] As funding agencies have begun to impose a requirement for investigators to share data resulting from funded research, the scale and scope of shared neuroscience data are expected to grow substantially.[23]

[12] Nicole Minielly et al., *Privacy Challenges to the Democratization of Brain Data*, 23 iScience (2020).

[13] Ienca et al., *supra* note 9.

[14] Eke et al., *supra* note 2, at 602.

[15] International Neuroimaging Data-Sharing Initiative, http://fcon_1000.projects.nitrc.org (accessed Apr. 5, 2022).

[16] OpenNeuro, https://openneuro.org (accessed Apr. 5, 2022).

[17] Human Connectome Project, https://www.humanconnectome.org (accessed Apr. 5, 2022).

[18] Alzheimer's Disease Neuroimaging Initiative, https://adni.loni.usc.edu (accessed Apr. 5, 2022).

[19] The BRAIN Initiative, https://braininitiative.nih.gov (accessed Apr. 5, 2022).

[20] EBRAINS, https://ebrains.eu (accessed Apr. 5, 2022).

[21] U.K. Biobank, https://www.ukbiobank.ac.uk (accessed Apr. 5, 2022).

[22] Canadian Open Neuroscience Platform, https://conp.ca (accessed Apr. 5, 2022).

[23] National Institutes of Health (NIH), *Final NIH Policy for Data Management and Sharing* (2020). https://grants.nih.gov/grants/guide/notice-files/NOT-OD-21-013.html (accessed Apr. 5, 2022); National Institute of Mental Health (NIMH), *Notice of Data Sharing Policy for the National Institute of Mental Health* (2019). https://grants.nih.gov/grants/guide/notice-files/NOT-MH-19-033.html (accessed Apr. 5, 2022); The Brain Research Through Advancing Innovative Neurotechnologies (BRAIN) Initiative, *Notice of Data*

The increasing availability of neuroscience data, along with technological advances in tools and algorithms for big data analysis, has raised concerns about potential privacy risks associated with neuroscience data.

Recent scholarly discussion about privacy concerns around neuroscience data has stemmed from the unique characteristics of the data. Neuroscience data can be inherently identifiable. For example, structural MRI images of the brain contain sufficient information about the unique folding structures of the brain to allow accurate matching of one image to another image of the same individual. In addition, structural MRI images also often include facial or skull features that may allow some degree of reidentification. Individually distinctive patterns of brain activation in functional data can be used to single out whom the data pertains to.[24] Analysis on neuroscience data can reveal data subjects' current health condition (eg whether the subjects have a brain tumor) and may allow estimation of the future risk of developing a neuropsychiatric disease (eg Alzheimer's disease[25] and Parkinson's disease[26]). Linking neuroscience data with information from another source, such as a publicly available demographic database, could unveil the subjects' identities, leading to disclosure, and potential misuse, of this sensitive health information,[27] although, as yet, no reports of any actual cases of this risk have materialized. Neuroscience data are also often combined and stored with other personal data, for example, genetic information or other medical, cognitive, behavioral test results. Thus, identifying subjects of neuroscience data could also result in uncovering these other personal data.

In addition to these aforementioned characteristics, researchers have also argued that neuroscience data are particularly more sensitive than are other personal or health data due to their intimate nature. Neuroscience data are considered to have philosophical relevance and moral importance to one's identity.[28] Because neuroscience data are more proximal to personhood compared with other data, they may unveil one's 'subconscious tendencies and biases' that are not filtered through executive control.[29] Others have claimed that neuroscience data could implicate mental privacy or freedom of thought because they can be used to decode mental contents in the brain, which has been the last fortress of mental privacy.[30] For example, recent studies have shown that it is possible to infer visual content of mental processing,[31] imagined handwriting,[32] or

Sharing Policy for the BRAIN Initiative (2019). https://grants.nih.gov/grants/guide/notice-files/NOT-MH-19-010.html (accessed Apr. 5, 2022).

[24] Vikram Ravindra, Petros Drineas, & Ananth Grama, *Constructing Compact Signatures for Individual Fingerprinting of Brain Connectome,* 15 Front Neurosci. (2021).

[25] Yong et al., *supra* note 6.

[26] Trina Mitchell et al., *Emerging Neuroimaging Biomarkers Across Disease Stage in Parkinson Disease: A Review,* 78 JAMA Neurol. 1262 (2021).

[27] Vikram Ravindra & Ananth Grama, *De-anonymization Attacks on Neuroimaging Datasets,* arXiv:1908.03260 (2019).

[28] Ienca & Androno, *supra* note 8; B. Tyer Fothergill, William Knight, Bernd C. Stahl, & Inga Ulnicane, *Responsible Data Governance of Neuroscience Big Data,* 13 Front Neuroinform. (2019).

[29] Goering et al., *supra* note 9, at 371.

[30] *Supra* note 8.

[31] Haiguang Wen et al., *Neural Encoding and Decoding with Deep Learning for Dynamic Natural Vision,* 28 Cereb. Cortex 4136 (2018).

[32] Francis R. Willett et al., *High-performance Brain-to-Text Communication via Handwriting,* 593 Nature 249 (2021).

covert speech[33] from neuroscience data. Although speculative, it has also been reported that neuroscience data can be used to predict a future tendency to carry out certain acts (eg criminal tendency).[34] Analysis on other types of personal or behavioral data are known to be able to provide precise and reliable assessment and prediction of one's mental states or behaviors,[35] but inferences from neuroscience data are viewed as especially sensitive because neuroscience data are more direct correlates of cognitive and affective states.[36] Furthermore, advancement in neuromodulation technology, such as BCI and transcranial magnetic or electrical stimulation, could also potentially violate the right to control one's thoughts and lead to manipulation of one's sense of agency or personal identity.[37] Yet, this risk reflects another aspect of privacy—freedom from intrusion or mental integrity—different from protection of information, which is the focus of the present article. Finally, commercialization of neuroscience data resulting from the emergence of neural devices and applications in the consumer domain is expected to increase the privacy risks associated with neuroscience data.[38]

III. PROPOSED POLICY AND REGULATORY APPROACHES FOR NEUROSCIENCE DATA PROTECTION

The unprecedented growth in the scale and scope of neuroscience data coupled with the increased awareness of the sensitive nature of the data has spurred extensive discussions on neuroscience data privacy and relevant data governance issues. Researchers have criticized the current regulatory framework, stating that it does not provide sufficient protection for neuroscience data and have proposed policy and regulatory approaches to better safeguard neuroscience data. First, it is argued that more granular consent should be required for neuroscience data.[39] In general, individual consent is the principal mechanism used to regulate personal information. Considering the potential privacy risks associated with neuroscience data, researchers have claimed that individuals, including research participants and consumers of neural devices, must be fully informed not only about the collection and processing of their data but also about sharing and reprocessing of the data.[40] Consent for neuroscience data should be specific to include what information will be collected from the subjects and who will do the collecting, for how long, and for what purpose.[41] Consent should also describe relevant potential risks, the process to revoke consent, and security measures employed to protect the data.[42]

[33] Dipti Pawar & Sudhir Dhage, *Multiclass Covert Speech Classification Using Extreme Learning*, 10 Machine Biomed. Eng. Lett. 217 (2020).

[34] *Supra* note 7.

[35] Nicole Martinez-Martin, Henry T. Greely, & Mildred K. Cho, *Ethical Development of Digital Phenotyping Tools for Mental Health Applications: Delphi Study*, 9 JMIR Mhealth Uhealth e27343 (2021).

[36] Giulio Mecacci & Pim Haselager, *Identifying Criteria for the Evaluation of the Implications of Brain Reading for Mental Privacy*, 25 Sci. Eng. Ethics 443 (2019).

[37] Yuste et al., *supra* note 8; Goering et al., *supra* note 9; Jan-Christoph Bublitz, *My Mind Is Mine!? Cognitive Liberty as a Legal Concept*, in Cognitive Enhancement: An Interdisciplinary Perspective (Elisabeth Hildt & Andreas G. Franke eds., 2013).

[38] Eke et al., *supra* note 2.

[39] Goering et al., *supra* note 9.

[40] *Id.*

[41] *Id.*

[42] *Id.*

The need for specific and transparent consent would be more critical in the commercial domain whereby data privacy is operated solely under an agreement between a consumer and commercial entity (eg terms of use (ToUs) or end-user license agreement (EULAs)) without additional oversight, such as the IRB review on human subject research under the Common Rule in the USA.[43] The US Federal Trade Commission (FTC) has authority to oversee data privacy in the consumer domain through section 5(a) of the FTC Act, which prohibits unfair and deceptive acts or practices in or affecting commerce.[44] The FTC has required companies to adhere to their privacy policies and employ reasonable data security measures and has taken enforcement action against the companies for failing to do so.[45] However, given the complex terms in ToUs or EULAs of direct-to-customer (DTC) neural devices currently on the market, such as EEG neurofeedback or transcranial electrical stimulation (tES) devices,[46] it might be difficult for ordinary consumers to give meaningful and specific consent to the collection, use, and transfer of their neuroscience data. Thus, it is argued that commercial sharing and sale of neuroscience data should be substantially limited.[47] Stringent restrictions on the commercial collection and processing of personal data under the European General Data Protection Regulation (GDPR) and California Consumer Privacy Act may provide useful models to enhance protection of neuroscience data in the commercial domain.[48] Furthermore, Goering and colleagues have also suggested that for neuroscience data, obtaining consent should be a dynamic process, and it should become a norm to revise consent over time to review unanticipated future use of the data. According to Goering and colleagues, '[g]reater granularity in consent gives the individual a broader axis of control, even if it creates a greater burden on participation'.[49]

In addition, researchers have been urged to adopt more rigorous deidentification methods to reduce the privacy risk. In the USA, collection, processing, and sharing of deidentified neuroscience data are not subject to regulatory requirements and limitations. When identifiable information is redacted from data, secondary research on the data may not fall under the definition of human subject research under the Common Rule, and deidentified data can be shared and analyzed without data subjects' new consent or additional IRB review.[50] The Health Insurance Portability and Accountability

[43] 45 C.F.R §46.109 (2018); Goering et al., *supra* note 9.

[44] 15 U.S.C. §45 (1994).

[45] Deven McGraw & Kenneth D. Mandl, *Privacy Protections to Encourage Use of Health-Relevant Digital Data in a Learning Health System*, 4 NPJ Digit. Med. (2021).

[46] See, eg, Insight from EMOTIV, https://www.emotiv.com/insight (accessed Apr. 5, 2022); Mindwave from NeuroSky, https://store.neurosky.com/pages/mindwave (accessed Apr. 5, 2022); Halo, https://www.haloneuro.com (accessed Apr. 5, 2022); LIFTiD, https://www.getliftid.com/index.html (accessed Apr. 5, 2022).

[47] Yuste et al., *supra* note 8; Goering et al., *supra* note 9.

[48] Regulation 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), 2016 0.J. (1. 119) 1 (EU); Cal. Civ. Code §1798.100, et seq. (2018).

[49] Goering et al., *supra* note 9, at 379.

[50] 45 C.F.R. §46.104(d)(4) (2018); Office of Human Research Protections (OHRP), *Coded Private Information or Specimens Use in Research, Guidance* (2008). https://www.hhs.gov/ohrp/regulations-and-policy/guidance/research-involving-coded-private-information/index.html (accessed Apr. 5, 2022).

Act (HIPAA) also prohibits the use or disclosure of personal health information by a covered entity (eg health plans, healthcare clearing houses, and healthcare providers) except in special circumstances.[51] Yet, HIPAA also does not restrict the use or disclosure of health information when it is deidentified—either by removing certain direct identifiers or by obtaining expert determination as to an extremely low statistical risk to identifying individuals using the information.[52]

However, there has been a growing concern on the adequacy and validity of conventional methods used to deidentify neuroscience data. For example, for neuroimaging data, it has been thought that removing or blurring facial features in the structural MR images, along with deleting direct identifiers in the metadata, is sufficient to prevent tracing back to an individual subject from the data.[53] Recent studies have shown that subjects' faces can be reconstructed from defaced structural images using AI and machine learning techniques, which may allow reidentification of the subjects.[54] Advances in statistical modeling may also increase the likelihood of reidentification even when deidentified datasets are substantially incomplete.[55] Thus, it is argued that additional procedures should be employed to deidentify neuroscience data, such as encryption of data with objective and verifiable blockchain tracking and processing of data through federated learning rather than using centralized processing.[56]

Some researchers have also recommended strictly controlled access to neuroscience data. For example, Eke and colleagues proposed that access to neuroimaging data for research purposes, even when deidentified, should be granted by project-specific or infrastructure-level data access review committees or a data access committee (DAC), which evaluates data requests and screens applicants who have requested the access.[57] They further argued that additional measures, such as data use agreements, should also be implemented to share neuroscience data.

Moreover, some scholars proposed a new rights-based approach in protecting neuroscience data privacy. They endorsed neurorights—rights to mental privacy or liberty against unwanted recording or manipulation of brain activity—to be incorporated into the existing human rights framework.[58] They further advocated for adopting a new regulatory system derived from neurorights that governs how to collect, process, and share neuroscience data. Yet, it should be noted that internationally acknowledged

[51] U.S. Department of Health and Human Services (HHS), *Summary of the HIPAA Privacy Rule* (2003). http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf (accessed Apr. 5, 2022).

[52] 45 C.F.R. §§164.514(a), (b) (2013).

[53] Mikhail Milchenko, *Obscuring Surface Anatomy in Volumetric Imaging Data*, 11 Neuroinformatics 65 (2013); Amanda Bischoff-Grethe et al., *A Technique for the Deidentification of Structural Brain MR Images*, 28 Hum. Brain Mapp. 892 (2007).

[54] David Abramian & Anders Eklund, *Refacing: Reconstructing Anonymized Facial Features Using GANs*, IEEE 16th International Symposium on Biomedical Imaging 1104–1108 (2019); Christopher G. Schwarz et al., *Identification of Anonymous MRI Research Participants with Face-Recognition Software*, 381 N. Engl. J. Med. 1684 (2019); Christopher G. Schwarz et al., *Changing the Face of Neuroimaging Research: Comparing a New MRI De-Facing Technique with Popular Alternatives*, 231 Neuroimage 117845 (2021).

[55] Luc Rocher, Julien M. Hendrickx, & Yves-Alexandre de Montjoye, *Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models*, 10 Nat. Commun. 3069 (2019).

[56] Eke et al., *supra* note 2; Yuste et al., *supra* note 8; Goering et al., *supra* note 9.

[57] Eke et al., *supra* note 2.

[58] Ienca & Andorno, *supra* note 8; Yuste et al., *supra* note 8; Goering et al., *supra* note 9.

human rights do not directly translate into actual, on the ground, legal or constitutional protections.

IV. MOVING BEYOND DATA PROTECTION

The primary rationale behind the proposed heightened policy and regulatory protection for neuroscience data largely focuses on potential future risks. Although a regulatory framework should account for the future prospect of technological advancement, a realistic assessment of state-of-the-art technology would be necessary to prevent unfounded hype, or fear, about the capacity of neuroscience data to read minds or predict specific outcomes.[59] Despite the alarming speculation on what can be inferred from neuroscience data, it remains far from reliably decoding complex cognitive and affective states.[60] Much of the previous work on predicting future outcomes using neuroimaging data also suffers from small sample sizes and extremely high rates of false positives;[61] the real-world accuracy of prediction of uncommon phenotypes (such as psychopathy) outside experimental settings is also heavily overestimated in studies that compare groups of equal sizes.[62] In addition, reports of substantial inconsistency among the studies on brain stimulation techniques (eg TMS and tES) have raised skepticism about the reproducibility of the findings and the efficacy of these techniques.[63] In terms of DTC neural devices and applications, only a small subset of neural devices can actually be (or have been) used in the consumer domain given the current state of technology and other relevant factors, such as costs or the need for a clinician's intervention in administering the devices. The systems available for consumer use also generally produce data of much lower quality than do research systems.[64]

In addition, scant evidence supports the impending risk of reidentification of individuals' neuroscience data and illicit disclosure of sensitive information within the data. As noted above, advances in novel software tools and algorithms to reidentify neuroscience data, such as facial reconstruction and functional brain fingerprinting, have called the validity of commonly used deidentification methods in neuroscience data into question. Nevertheless, these tools and algorithms are still at an exploratory stage and have only been used for demonstration purposes,[65] and to date, there has been no evident surge in attempts to reidentify neuroscience data or to abuse sensitive information in the data to harm subjects.

It is also not clear whether, at least given the current state of technology, privacy risks are more salient in neuroscience data compared with other sensitive personal data. It seems that the special characteristics of neuroscience data that have been argued to warrant more rigorous protection are conceptual or philosophical rather than functional (eg what information can be inferred or extracted from the data). Other types of personal or biometric data, such as internet search history, GPS tracking,

[59] Choudhury et al., *supra* note 2.

[60] Hosseini et al., *supra* note 11; Poldrack, Huckins, & Varoquaux, *supra* note 11.

[61] Poldrack, Huckins, & Varoquaux, *supra* note 11; Varoquaux, *supra* note 11.

[62] Poldrack, Huckins, & Varoquaux, *supra* note 11.

[63] See, eg, Martin E. Héroux et al., *Questionable Science and Reproducibility in Electrical Brain Stimulation Research*, 12 Plos One (2017); Lauren E. Mancuso et al., *Does Transcranial Direct Current Stimulation Improve Healthy Working Memory?: A Meta-analytic Review*, 28 J. Cogn. Neurosci. (2016).

[64] Anna Wexler, *Separating Neuroethics from Neurohype*, 37 Nat. Biotechnol. 988 (2019).

[65] *Supra* note 54.

behaviors on social networking platforms, and digital health device/application data, are known to be able to provide highly accurate and sensitive information about individuals (eg one's personality, political preference, or future health conditions). Measuring behavior or other health indicators from these data is called digital phenotyping.[66] For example, Kosinski and colleagues were able to predict nearly all of the explainable variance in the personality trait of openness by analyzing Facebook likes. The supposedly intimate nature of neuroscience data—they are more proximal to one's identity and more directly correlated with cognitive and affective states—might have philosophical importance, but it would be difficult to claim that inferences on individuals based on neuroscience data are more powerful than those based on other types of personal data.[67] In fact, behavioral or digital phenotyping data are often combined with neuroscience data and are necessary to draw and support inferences from neuroscience data.

More importantly, even though privacy is a critical individual interest, it is not without limits. Developing a policy or regulatory framework on neuroscience data thus requires a rigorous balancing of risk to an individual's privacy and the societal benefits of collection and sharing of neuroscience data. However, the policy and regulatory approaches proposed in the literature are heavily skewed toward restricting collection, access to, and sharing of neuroscience data and may impose a substantial burden on conducting neuroscience research. For example, specific and granular consent would be quite challenging to obtain for secondary research on deidentified data because it is nearly impossible to foresee precisely what kind of analyses will be conducted on the data. In fact, these analyses might not yet have been developed or even conceived of at the time of initial data collection. In addition, tracking subjects of deidentified data to obtain consent for secondary research would be not only onerous but also ethically impermissible because it requires reestablishing the subjects' identity, which was promised to be kept undisclosed.

Different consent mechanisms have been suggested to address these issues. For example, dynamic consent refers to a personalized digital communication interface to allow research subjects to consent to new projects or to update their consent preferences in real time.[68] Data trust is another example,[69] whereby subjects delegate to data trustee(s) the responsibility to determine what type of data processing aligns with subjects' interests. However, there remain practical challenges and technical bottlenecks in implementing these mechanisms. In this regard, it would be worth noting that there have been efforts to develop generic consent forms that embody the idea of broad consent for open data sharing while providing adequate protection for subjects' privacy, such as Open Brain Consent.[70]

[66] Martinez-Martin, Greely, & Cho, *supra* note 35.

[67] Michal Kosinski, David Stillwell, & Thore Graepel, *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*, 110 Proc. Natl. Acad. Sci. 5802 (2013).

[68] Karen Spencer et al., *Patient Perspectives on Sharing Anonymized Personal Health Data Using a Digital System for Dynamic Consent and Research Feedback: A Qualitative Study*, 18 J. Med. Internet Res. e66 (2016); Jane Kaye et al., *Dynamic Consent: A Patient Interface for Twenty-First Century Research Networks*, 23 Eur. J. Hum. Genet. 141 (2015).

[69] UK AI Council, *Exploring Legal Mechanisms for Data Stewardship* (2021). https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/ (accessed Apr. 5, 2022).

[70] Elise Bannier et al., *The Open Brain Consent: Informing Research Participants and Obtaining Consent to Share Brain Imaging Data*, 42 Hum. Brain Mapp. 1945 (2021).

If not carefully calibrated to the sensitivity of data, stringent access control and limitations on subsequent use of data—at various levels (eg individual project, institutional, data archive, funding agency, national and international level)—could also have chilling effects on data sharing and hamper open access to data. For example, it is argued that review by DACs could adversely influence access to data due to potential conflicts of interest of data contributors when they are involved in DACs management.[71]

The proposed policy and regulatory restrictions seem to focus on neuroscience data in the commercial domain, but sometimes the line between neuroscience data collection and processing for commercial purposes and that done for research (or clinical) purposes can be blurry. How to draw a distinction between research and clinical data and whether and how they should be treated differently under the proposed policy and regulatory requirements have not been explicitly addressed, and these uncertainties could have adverse spillover effects on research and clinical contexts.

Furthermore, complete privacy may not be a realistic expectation in the era of AI and big data analytics. Even with the best available privacy and security measures, including cutting-edge deidentification tools suggested in the literature, it would be impossible to *completely* eliminate the risks of reidentification and unwanted disclosure of neuroscience data. If this remaining risk was to materialize, however, unlikely given the current state of technology, it could potentially cause detrimental harm to subjects. It is also important to note that disclosure of neuroscience data and related sensitive information per se would rarely cause harm, although it might make subjects feel vulnerable or distressed. This dignitary harm is difficult to identify, and it is also not generally recognized as a damage entitled to a legal remedy in data breach cases under the standing jurisprudence.[72] Rather, more concrete harm would result from the use of neuroscience data or information inferred from the data with an intent to put the subjects in peril, as in the cases wherein a subject's disease biomarker or personality traits derived from neuroscience data are used to discriminate against the subject (eg in employment or health insurance context).

Therefore, ideally, a regulatory scheme to address privacy risks of neuroscience data should go beyond data protection and also prevent potential harm. In other words, policy and regulatory efforts should not solely focus on controlling access to and disclosure of data but also focus on minimizing the opportunities for the data to be used in ways that could harm data subjects.[73,74] We propose that along with other reasonable privacy

[71] Mahsa Shabani et al., *Controlled Access under Review: Improving the Governance of Genomic Data Access*, 13 PLoS Biol. e1002339 (2015).

[72] George Ashenmacher, *Indignity: Redefining the Harm Caused by Data Breaches*, 51 Wake Forest L. Rev. 1 (2016).

[73] McGraw & Mandl, *supra* note 44; Carolyn R. Chapman et al., *Genetic Discrimination: Emerging Ethical Challenges in the Context of Advancing Technology*, 7 J. L. Biosci. (2020).

[74] Forbidding reidentification of neuroscience data could be another way to protect individuals to whom the data pertains from potential informational or discriminatory harm (Michael J. S. Beauvais, Bartha M. Knoppers, & Judy Illes, *A Marathon, Not a Sprint - Neuroimaging, Open Science and Ethics*, 236 Neuroimage 118041 (2021)). For example, the Data Protection Act in the UK has a provision that makes knowingly or recklessly reidentifying information that is deidentified personal data without the consent of the controller responsible for deidentifying the data illegal (2018, Sec 171). This can be more effective than other existing mechanisms, such as data use agreements, which are private agreements between researchers or a researcher and a data repository (Michael J. S. Beauvais, Bartha M. Knoppers, & Judy Illes, *A Marathon, Not a Sprint - Neuroimaging, Open Science and Ethics*, 236 Neuroimage 118041 (2021)). However, creating

and security measures, new legislation that prohibits misuse of neuroscience data would provide the ultimate safeguard against potential harm associated with the data, without unnecessarily limiting the use of neuroscience data, to foster an understanding of brain function in an effort to prevent and treat brain disorders.[75]

V. LEARNING FROM THE GINA: DEVELOPING A REGULATORY SAFEGUARD AGAINST THE MISUSE OF NEUROSCIENCE DATA

Building a new regulatory regime against the misuse of neuroscience data would require substantial combined efforts and inputs from various stakeholders, including policy makers, lawyers, bioethicists, neuroscientists, industry leaders, and the general public. Scoping the entire landscape of these efforts is beyond the purview of this article, but as an attempt to guide future discussions between these stakeholders, here we examine some of the core questions that need to be addressed in developing this regulatory regime.

In fact, how to protect individuals from potential harmful use of sensitive information is not a new issue, and regulatory actions have been taken in other contexts. One particularly relevant regulatory model is the GINA. The GINA is a US federal regulation that prohibits discrimination by health insurers and employers on the basis of genetic information. Other laws and regulations partially provide protections against genetic discrimination, but GINA is the first to set a federal standard necessary to prevent discriminatory and adverse treatment of asymptomatic individuals based on their or their relative's actual or presumed genetic characteristics.[76]

Similar to neuroscience data, genetic data have been considered inherently sensitive information. DNA has been 'conceptualized as a unique identifier and a person's book of life, which provides insights into many aspects of current and future propensities for diseases and behavior', although the amount, detail, and significance of private information that DNA sequences can reveal might be vastly overestimated.[77] The fact that the genetic sequence is immutable and contains information about family members (and possibly others with shared ancestry) adds another layer of sensitivity. This conceptualization raised a need for a strong regulatory safeguard against discriminatory use of genetic information. In addition, when the GINA was enacted, no strong empirical evidence of ongoing or expected genetic discrimination existed. However, survey data did show that a significant number of people expressed fear that they might suffer from genetic discrimination should their genetic information become available to other individuals or entities.[78] Legislatures were worried that this fear of genetic discrimination might prevent people from participating in genetic research or from

legal prohibition on misuse of neuroscience data would provide stronger protection for data subjects than would prohibition on reidentification.

[75] Jwa & Poldrack, *supra* note 1.

[76] Cheryl Erwin, *Legal update: Living with the Genetic Information Nondiscrimination Act*, 10 Genet. Med. 869 (2008).

[77] Ellen W. Clayton et al., *The Law of Genetic Privacy: Applications, Implications, and limitations*, 6 J. L. Biosci. 1, 2 (2019).

[78] Joanne Barken, *Judging GINA: Does the Genetic Information Nondiscrimination Act of 2008 Offer Adequate Protection*, 75 Brooklyn L. Rev. 545 (2009); Nancy E. Kass et al., *Access to Health Insurance: Experiences and Attitudes of Those with Genetic versus Non-Genetic Medical Condition*, 143A Am. J. Med. Genet. A. 707 (2007).

seeking genetic testing when needed for their healthcare. The GINA is intended to address this fear factor, which echoes the concerns with respect to neuroscience data, by forbidding discriminatory use of genetic information in insurance and employment settings, allowing individuals to take advantage of genetic testing, technologies, research, and new therapies.[79] Therefore, GINA would provide a useful reference to the new legislation we propose. In the following analysis, we will examine the core regulatory questions regarding the new legislation on the basis of what we have learned from the enactment of the GINA and the merits and weaknesses of the protection it provides.[80]

V.A. Why Do We Need a Regulatory Safeguard Specifically Targeted At Misuse of Neuroscience Data?

Neuroscience data are considered uniquely sensitive. However, as discussed above, these unique features are based on conceptual and philosophical values, and given the current state of technology, it would be difficult to say that neuroscience data hold a special status compared with that of personal or health data in terms of what information can be inferred from the data. In other words, information derived from personal or health data can be as harmful as that from neuroscience data when used by individuals or entities with malicious intent against the data subject. One can then raise a question as to why we should have legislation that specifically targets the misuse of neuroscience data.

The GINA was first introduced in 1995 in response to advances in genetic research to decipher the human genome sequence and the genetic basis of illness along with the expected substantial increase in the amount of genetic testing being done. Before GINA, about 40 states had their own laws against genetic discrimination in health insurance and employment contexts, which showed that introducing new legal prohibitions could occur without causing major harm to health insurers or employers and created some desire for a uniform federal law to avoid conflicting state laws. These state-level laws were expected to make passage of the federal law easier, but it still took 13 years of legislative efforts to pass the bill. During the 10-plus years of legislative maneuvering to enact GINA, intensive debate arose over whether genetic information should be treated the same as other sensitive health information was or whether the distinctive conceptualization of genetic information requires separate and more heightened protection.[81] As in the case of neuroscience data, people tend to mystify genetic data and consider them as exceptionally revealing, and thus, particularly sensitive, although such data may not have fundamentally different potential compared with other personal data. On the other hand, there was strong criticism of this genetic exceptionalism, which

[79] 42 U.S.C. §2000ff (4) (2008); Yann Joly et al., *Looking Beyond GINA: Policy Approaches to Address Genetic Discrimination*, 21 Annu. Rev. Genomics Hum. Genet. 491 (2020).

[80] Other researchers have also argued for a need to prevent misuse of neuroscience data and laid out regulatory proposals similar to the GINA. However, these proposals have a rather narrow scope focusing on a specific context, for example, employment (Stephanie A. Kostiuk, *After GINA, NINA? Neuroscience-based Discrimination in the Workplace*, 65 Van. L. Rev. 933 (2012)), health insurance (Joyce J. Shin, *Closing the Gap: Protecting Predictive Neuroscience Information from Health Insurance Discrimination*, 64 Emory L.J. 1433 (2015)), or law enforcement (Nita Farahany, *Incriminating Thoughts*, 64 Stan. L. Rev. 351 (2012)). Here we aim to provide a more comprehensive analysis that examines fundamental core regulatory questions not limited to a certain context.

[81] *Supra* note 77.

could in fact exacerbate genetic discrimination or stigma by highlighting the *specialness* of genetic information.[82] Clayton and colleagues suggested that the principle reason we have genetic-specific law, both at the federal and state level, despite the criticism of genetic exceptionalism, is because 'genetic-specific laws are necessarily narrower in scope and are thus more likely to garner political support'.[83]

A broad piece of legislation encompassing different types of sensitive personal information—focusing on capability of data rather than types of data—would be ideally suited for comprehensive protection against the misuse of the information. Yet, at the same time, it would be overly inclusive and challenging not only to enact and but also to enforce. The European Union's GDPR is one example of extensive data protection law, although its protection is not limited to misuse of data. Its sweeping restrictions on processing of any types of personal data reset the standard of data protection but left substantial uncertainties. Particularly relevant to our analysis are ambiguities regarding conditions and requirements for legitimate processing of personal sensitive data for a research purpose.[84] Recent futile attempts to enact federal privacy legislation on consumer data in the USA also showed how difficult it would be to reach an agreement to pass a broad bill given the partisan polarization in Congress.[85] Neuroscience data-specific regulatory protection, such as *Neuroscience Information Nondiscrimination Act*, would likely be an inevitable compromise akin to the GINA. It could be justified by the relatively large gap between a realistic level of privacy risk and anticipatory apprehension in neuroscience data along with this gap's potentially detrimental effects on advancing neuroscience research.

V.B. Why can't We Just Extend Existing Regulatory Protections to Neuroscience Data?

Enacting new legislation is an arduous process that requires extensive efforts in navigating varying political and social landscapes and in forming a consensus on how to balance societal and individual rights and interests for the given regulatory issue. Thus, it can be argued that extending or amending existing laws and regulations to include neuroscience data under their protections would be a more practical and viable option by which to achieve needed safeguards against the abuse of neuroscience data.

As noted earlier, GINA was not the first legislative action that aimed to address discrimination on the basis of genetic information. Other laws and regulations were already in effect before GINA that either specifically address or could be extended to genetic discrimination, but there were significant gaps in these patchworks of federal and state protections. For example, HIPAA has provisions that restrict the use of preexisting health conditions, including genetic information, in setting premiums and determining eligibility for insurance benefits, but only in group health plans.[86] In

[82] *Id.*

[83] *Id.* at 8.

[84] Robert Eiss, *Confusion over Europe's Data-Protection Law Is Stalling Scientific Progress*, 584 NATURE 498 (2020); David Peloquin et al., *Disruptive and Avoidable: GDPR Challenges to Secondary Research Uses of Data*, 28 EUR. J. HUM. GENET. 697 (2020).

[85] David McCabe, *Congress and Trump Agreed They Want a National Privacy Law. It Is Nowhere in Sight*, THE NEW YORK TIMES, Oct. 1, 2019.

[86] Chapman et al., *supra* note 72; U.S. Department of Labor, *Employee Benefits Security Administration, FAQs on HIPAA Portability and Nondiscrimination Requirements for Workers*, https://www.dol.gov/sites/default/files/ebsa/about-ebsa/our-activities/resource-center/faqs/hipaa-consumer.pdf (accessed Apr. 5, 2022).

the employment context, the Americans with Disabilities Act (ADA) can be applied if genetically related illness reaches the level of disability by substantially limiting a major life activity.[87] The ADA also affords protection when an employer has perceived an employee to be disabled even though he or she is not in fact limited in ability to perform work.[88] Yet, this standard is often difficult to prove, and it is not clear whether having a genetic predisposition to develop a disease in the future meets the definition of perceived disability under the ADA.[89] Other regulations applicable to the employment context—Executive Order 13,145 that limits access to and use of employees' genetic information[90] or the Privacy Act of 1974[91] that governs employees' private records more generally—also fall short of providing adequate protection due to their limited scope that covers only federal employees. In addition, state laws against genetic discrimination provide varying levels of protection. Thus, GINA was required to fill these gaps and to set the nationwide standard against genetic discrimination.

Some of these existing regulatory protections could be extended to the use of neuroscience data for discriminative purposes, such as the ADA or the Privacy Act of 1974, for adverse employment actions. It was also argued that amending the Patient Protection and Affordable Care Act (ACA) could be an easier path to follow to prevent misuse of neuroscience data in the health insurance context, particularly regarding predictive information derived from neuroscience data.[92] The ACA was enacted in 2010 in part to broaden the restrictions on the use of preexisting conditions in the health insurance context under HIPAA and to reinforce GINA's protection for asymptomatic individuals by barring health insurers from discriminating on the basis of health status, which includes predictive genetic information.[93] Expanding the ACA's protection to neuroscience data would be possible by adding predictive neuroscience information as a health status under the act.[94] However, these approaches would cover only limited contexts (eg either employment or the health insurance context) under certain conditions (eg when a manifested brain-related illness reaches the level of disability or when employers are federal departments or agencies) and would still leave gaps and uncertainties. Although it would require more resources and effort, building new overarching legislation would be desirable to ensure comprehensive and consistent protection, which would include making needed amendments in relevant existing laws and regulations similar to what was found in GINA.

V.C. How should We Define Neuroscience Information for the New Regulatory Protection?

The first step in developing new legislation would be crafting a clear definition of core concepts. Earlier, we defined neuroscience data—or brain data—following Eke and colleagues,[95] as raw measurements of nervous system structure, activity, and function

[87] 42 U.S.C. §12102(1) (1990).

[88] 42 U.S.C. §§12102(1), (3) (1990).

[89] *Supra* note 78.

[90] 65 Fed. Reg. 6877 (2000).

[91] 5 U.S.C. § 552a(b) (1974).

[92] Shin, *supra* note 80.

[93] 42 U.S.C. §300gg–4 (2010).

[94] Shin, *supra* note 80.

[95] Eke et al., *supra* note 2.

along with derived data and metadata describing the processing steps and analyses used to generate derived data. For the new legislation, we propose *Neuroscience Information Nondiscrimination Act*, neuroscience information refers to information on an individual's past, present, and future health condition, cognitive state, or behavioral trait directly inferred from neuroscience data. Under the GINA, only predictive genetic information—genetic information of asymptomatic individuals—is protected from misuse. This limited coverage of the GINA had been criticized until the ACA was introduced to pick up where the GINA had left off and expand the protection, at least in the health insurance context, to those who had already manifested diseases or health conditions under the ACA's preexisting condition provision.[96] Reflecting on the GINA's limitation, it seems the new regulatory safeguard should encompass misuse of previous, current, or predictive information about an individual based on neuroscience data so that the safeguard could provide more comprehensive protection.

The GINA's definition of genetic information extends beyond a person's genetic tests to include genetic tests or manifestation of a disease or disorder of the person's family members (up to and including fourth-degree relatives).[97] In addition to the genetic test results, the fact that a person or his or her family members participated in 'research that includes genetic testing, counseling, or education' also falls under the definition of genetic information.[98] Some neurological or psychiatric disorders (eg Parkinson's diseases or Alzheimer's disease) are known to have a genetic basis,[99] and thus the information that an individual has a brain-based biomarker for these disorders can be used not only to infer a likelihood of developing these diseases but also to infer the same for the person's close relatives.[100] The GINA already provides protection for manifestation of these neurological or psychiatric disorders in close relatives. However, we would want to go further and include nongenetic brain-based biomarkers of the individual's close relatives, such as neuroimaging biomarkers, under the new regulatory protection so that this person could be safeguarded against the harmful use of that information. Given that participation in a neuroscience research study (eg research on preclinical Alzheimer's disease or depression) in and of itself could implicate an individual's health condition, cognitive state, or behavior, this information should also be protected along with other neuroscience data, as occurs in the GINA.

V.D. In What Contexts Would We Want to Prohibit Misuse of Neuroscience Information?

Once we have formed a clear definition of neuroscience information, the next core question we should ask is how to delineate the scope of the legislation. That is, in what

[96] Kelly Rich, *Genetic Information Nondiscrimination Act and the Affordable Care Act: When Two Is Better Than One*, 22 Genet. Test. Mol. Biomark. 331 (2018).

[97] Here the term 'genetic test' means 'an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, that detects genotypes, mutations, or chromosomal changes (42 U.S.C. §2000ff (4)(A) (2008))'.

[98] 42 U.S.C. §2000ff (4)(B) (2008).

[99] See, eg, Lynn M. Bekris et al., *Genetics of Alzheimer Disease*, 23 J. Geriatr. Psychiatry Neurol. 213 (2010); Claudia Schulte & Thomas Gasser, *Genetic Basis of Parkinson's Disease: Inheritance, Penetrance, and Expression*, 4 Appl. Clin. Genet. 67 (2011); Caroline Van Cauwenberghe, Christine Van Broeckhoven, & Kristel Sleegers, *The Genetic Landscape of Alzheimer Disease: Clinical Implications and Perspectives*, 18 Genet. Med. 421 (2016).

[100] Young et al., *supra* note 6; Mitchell et al., *supra* note 26.

contexts and under what conditions should the misuse of neuroscience information be prohibited? There can be different regulatory options in answering this question; for example, enumerating specific contexts in which neuroscience information should not be used could be one option. The GINA followed this approach and restricted the use of genetic information in only two contexts, health insurance and employment.[101] Yet, it would also be possible to devise an overall prohibition with certain exceptions, as in the HIPAA Privacy Rule, which generally prevents the use and disclosure of protected health information, except in special circumstances listed in the rule (eg for treatment, payment, and healthcare operations or public interest and benefit activities).[102] Recently, GINA's approach has been criticized as insufficient, in part due to the substantial growth in the DTC genetic testing industry and resulting increased commercial transfer of genetic information outside research and clinical contexts.[103] It has been argued that GINA's protection should not be limited to health insurance and employment and that it should be amended to include the use of genetic information in other contexts, such as education and housing.[104] At the same time, although HIPAA's approach seems to provide more comprehensive protection, HIPAA only applies to covered entities, such as health plans or healthcare providers.[105]

Determining which regulatory approach would be desirable for the proposed new legislation would require careful deliberation on trade-offs between these options. Narrowing the scope of protection would enable regulatory resources to be directed to certain salient circumstances. Nevertheless, as with the GINA, this new legislation could well be considered myopic because it would not include potential misuse of neuroscience information in other contexts, especially given that the process of amending legislation is no less strenuous than is enacting new legislation. On the other hand, sweeping prohibitions across various possibilities might provide the utmost protection against the misuse of neuroscience information without the any need for future amendments. However, such legislation could become too vague to have meaningful enforcement effects without defining who should be subjected to the prohibition or what would constitute misuse or discriminatory use. Its scope might then need to be narrowed substantially, as in the case of HIPAA, which only applies to certain covered entities. In addition, carving out exceptions as to when and under what conditions neuroscience data can be lawfully used would be challenging considering the prohibition's broad scope. Here, we do not seek to resolve this question but will examine some of the contexts in which the use of neuroscience information may cause informational or discriminatory harm, on the basis of what we have learned from GINA, to inform future legislative discussion.

i. Health insurance

Under the GINA, group and individual health insurers are forbidden to use a person's genetic information in determining eligibility or setting coverage, underwriting, or

[101] California state lawmakers have expanded GINA's protections to cover emergency medical services, housing, mortgage lending, education, life insurance, elections, and state-funded programs. Pardeep Singh et al., *Increasing Use of Genetic Data Requires New Privacy Considerations*, 15 J. Sci. Policy Govern. 6. (2019).

[102] 45 C.F.R. §§164.502, 164.512 (2013).

[103] *Supra* note 77.

[104] *Id.*

[105] 45 C.F.R. §160.102 (2013).

setting premiums.[106] It also prevents health insurers from requesting a person's genetic information or requiring that a person undergo a genetic test.[107] However, collection of genetic information incidental to collection of other information does not violate the GINA.[108] The GINA amended other relevant laws and regulations to provide coherent protection. For example, it revised the HIPAA to include genetic information as protected health information, and therefore, use and disclosure of genetic information by covered entities for underwriting purposes is prohibited.[109]

As in the case of genetic information, there is a strong financial incentive on the health insurers' side to obtain and use a (potential) insured's neuroscience information, which can indicate the insured's health state, particularly regarding future health conditions. For example, as discussed earlier, neuroscience data could be used to derive a biomarker for a brain disorder, such as Alzheimer's disease. Advances in neuroimaging methods allow researchers to detect abnormal accumulation or tangles of certain proteins (eg amyloid or tau) in the brain, which are known to be associated with the risk of developing Alzheimer's disease.[110] The concentration of these proteins in cerebrospinal fluid in the brain and spinal cord can also predict an increased risk of Alzheimer's disease. However, unlike genetic risk factors of Alzheimer's disease (eg APOE4 gene or presenilin-1 mutation) protected under the GINA, the brain-based biomarkers derived from neuroscience data are currently left without protection despite their significant predictive value. Thus, health insurers should be barred from using neuroscience information to adjust group or individual premiums or deny coverage to individuals who have not yet manifested a disease or disorder that might have a neural basis evidenced in the neuroscience information.[111] Requiring or requesting neuroscience data or intentionally obtaining neuroscience data should also be illegal. Acknowledging that it is impossible to completely control the risk of disclosure, we might want to provide an exception similar to GINA's incidental collection. Nevertheless, as in GINA, discriminatory use of neuroscience information should be disallowed regardless of how health insurers obtained the information.

In addition, one of the major criticisms on GINA's protection in the health insurance context is that it does not include discrimination in the areas of life, disability, or long-term care insurance despite that the potential harm of discrimination in these types of insurance is as substantial as, if not greater than, is the harm in health insurance discrimination.[112,113] Although excluding these types of insurance from GINA was largely a

[106] Amanda K. Sarata & Jody Feder, *The Genetic Information Nondiscrimination Act of 2008 (GINA)*, Congressional Research Service Report (2015).

[107] *Id.*

[108] *Id.*

[109] 42 U.S.C. § 1320d-9 (2008).

[110] Andrei G. Vlassenko, Tammie L. S. Benzinger, & John C. Morris, *PET Amyloid-Beta Imaging in Preclinical Alzheimer's Disease*, 1822 Biochim. Biophys. Act. 370 (2012); La Joie et al., 2020. *Prospective Longitudinal Atrophy in Alzheimer's Disease Correlates with the Intensity and Topography of Baseline tau-PET*, 12 Sci. Transl. Med. (2020).

[111] As noted earlier, once a disease or disorder that might have a neural basis is manifested, the ACA protection that prevents health insurers from discriminating on the basis of preexisting condition would apply.

[112] Mark A. Rothstein, *Putting the Genetic Information Nondiscrimination Act in Context*, 10 Genet. Med. 655 (2008).

[113] Some states' laws on genetic discrimination do limit the use of genetic information by life, disability, and long-term care insurers (Jarrod O. Anderson, Anna C. Lewis, & Anya E. Prince, *The Problems with*

strategic decision to get the bill passed, it is also argued that there are legitimate reasons to treat these types differently from how health insurance is treated. Life, long-term care, and disability insurance are 'perceived as more optional and commercial' than is health insurance, which is necessary to obtain affordable access to healthcare.[114] Insurers have also claimed that preventing the use of genetic information for underwriting purposes would cause adverse selection—a tendency that high-risk individuals would disproportionately purchase insurance coverage, whereas low-risk individuals would drop out by taking the advantage of the informational asymmetry that information on genetic risk factors is only available to consumers.[115] Given that similar tension would arise regarding this new legislation, more discussion on how to balance appropriate protection for individuals with financial sustainability of the insurance industry would be needed.

ii. Employment

The GINA prohibits employers from using a person's genetic information in making employment decisions in hiring, discharging, or any other terms, conditions, or privileges of employment.[116] Employers are also prevented from requesting, requiring, or purchasing genetic information about persons or their family members. Again, GINA provides several exceptions to the prohibition on collection of genetic information.[117] For example, employees enrolled in employer-sponsored wellness programs may voluntarily or inadvertently disclose family history that indicates a risk of genetic disease.[118] However, employers are still not allowed to use the inadvertently obtained genetic information to discriminate against employees. Given that it could indicate not only employees' health conditions but also employees' cognitive states or behavioral traits, neuroscience information could have broader implications in the employment context compared with genetic information. Employers may find neuroscience information useful in screening their (potential) employees or in evaluating their work performance beyond just reducing health costs. For example, employers may want to monitor employees' attention levels or behavioral tendencies, even when it does not implicate any propensity to develop a disease or disorder, by collecting and analyzing neuroscience information, such as assessment of their EEG data. Moreover, on the basis of this information, employers may even want to modulate the employees' cognitive states or behaviors using neurotechnology (eg tES or TMS) to enhance their work performance.[119] Thus, following GINA's precedent, employers should be prohibited from willfully acquiring (potential) employees' neuroscience information and using it to make employment decisions that could adversely affect the employees.

Recently, some scholars raised a question regarding whether there could be potential beneficial use of genetic information in employment settings. For example, Chapman and colleagues argued that with the potential increase in accuracy and predictive power

Patchwork, State Approaches to Regulating Insurer Use of Genetic Information, 22 DePaul J. Health Care L. (2021)).

[114] Robert C. Green, Denise Lautenbach, & Amy L. McGuire, *GINA, Genetic Discrimination, and Genomic Medicine*, 372 N. Engl. J. Med. 397, 398 (2015).

[115] *Id.*

[116] 42 U.S.C. § 2000ff-1(a) (2008).

[117] 42 U.S.C. § 2000ff-2(b) (2008).

[118] Cheryl Erwin, *Behind the Genetic Information Nondiscrimination Act of 2008*, 109 Am. J. Nurs. 46 (2009).

[119] Kostiuk, *supra* note 80.

of genetic testing, it may become ethical and justifiable to use genetic information in making employment decisions, as special exceptions, if it is proved to be relevant to job performance and employee safety.[120] In the future, genetic information (eg genetic testing on viral resistance or seizure risk) may help us understand that individuals with certain genotypes would need specific accommodations to better perform their job duties or to protect themselves or others in the work environment.[121] Chapman and colleagues added that modifying the GINA to allow these exceptions should be granted only after rigorous social discussion and legislative deliberation.[122] Our knowledge on the neural basis of health conditions, cognitive states, and behavioral traits is still too rudimentary to make accurate and reliable inferences, but we may also want to contemplate whether the use of neuroscience information could be warranted to identify needed accommodations and support to protect employees or enhance their performance.

iii. Other potentially relevant contexts

Health insurance and employment would likely be the two most salient circumstances wherein the new legislation's protection should be accorded, but there are other contexts in which neuroscience information could be used for discriminative purposes and in which the harm caused by such misuse could be highly detrimental. Increasing availability of neuroscience information outside the research and clinical domain would lead to more unwanted disclosures and to the misuse of neuroscience information in these contexts, regardless of the information's accuracy and credibility. On the basis of the criticism of the GINA's limited scope, the new legislation should extend its protection against misuse of neuroscience information to these contexts. For instance, educational institutions, including primary, secondary, and higher education institutions, would have an interest in collecting and using applicants' or students' neuroscience information. This could have some implications on their future academic performance and social skills, for admissions, educational evaluation and placement, or disciplinary actions. Neuroscience information might also be used to discriminate against individuals in obtaining housing (eg purchasing, renting, or financing real estate), such as senior or assisted living communities that might want to know whether an applicant has a biomarker for developing a neurodegenerative disease in the future.[123]

Neuroscience information may also be considered useful in the legal system. It could be used for screening immigrants about their political or religious orientation in the immigration proceedings or for determining whether a parent is mentally capable of raising a child (eg psychiatric disorders, aggression level, propensity for substance and alcohol abuse) in a child custody proceeding. There has been extensive discussion on the potential controversial use of neuroscience information in law enforcement and criminal proceedings and the need for a statutory protection in this context.[124] For

[120] Chapman et al., *supra* note 73.

[121] *Id.*

[122] *Id.*

[123] Mark A. Rothstein & Laura Rothstein, *How Genetics Might Affect Real Property Rights: Currents in Contemporary Bioethics*, 44 J. L. Med. Ethics 216 (2016).

[124] Farahany, *supra* note 79; Sjors L. T. J. Ligthart, *Coercive Neuroimaging, Criminal Law, and Privacy: A European Perspective*, 6 J. L. Biosci. 289 (2019); Francis X. Shen, *Neuroscience, Mental Privacy, and the Law*, 36 Harv. J. L. Public Policy 653 (2013).

example, it could be used as evidence of whether a suspect or defendant has criminal capacity or possesses guilty knowledge in a trial. Judges at a bail hearing or parole hearing might want to know the risk of flight or recidivism, something that might be gleaned from neuroscience information. It may also be possible that the court would want to monitor or even modulate criminals' neural functioning for surveillance and rehabilitation purposes. However, it is important to note that there is strong public interest in law enforcement and criminal justice in our society. Thus, regulating the use of neuroscience in this context would require a more nuanced approach 'to strike a proportionate balance' between individual rights and societal interests.[125] Lawful use of neuroscience information, if any, should be drafted via democratic deliberation. Its use should be restricted to limited to settings in which rigorous procedural safeguards are implemented. Such safeguard might include, for instance, requiring court orders (eg warrant or subpoena) or limiting negative inferences from refusals to submit neuroscience information in criminal investigations or trials.[126]

V.E. How would this New Legislation Work?

Despite criticisms on its limited scope and application, GINA was indeed a critical step toward protection against genetic discrimination. To enforce the nondiscrimination requirements in the context of health insurance, GINA authorizes the secretary of Health and Human Services to impose penalties for noncompliance. Health plans and health insurance issuers who fail to meet the requirements are liable for a penalty of $100 per day in the noncompliance period per each participant or beneficiary to whom such failure relates.[127] For willful violation, GINA establishes a minimum penalty of $2500, or $15,000 for more severe or prolonged.[128] Individuals who believe that their employment rights have been violated on the basis of genetic information may file a complaint with the US Equal Employment Opportunity Commission (EEOC).[129] The EEOC will investigate the charge to determine whether there is 'reasonable cause' to believe discrimination occurred and may file a court action if the charge cannot be resolved through conciliation. A charging party may also file a lawsuit in federal court.[130] The remedies of the employment provisions of GINA generally track Title VII of the Civil Rights Act of 1964, which prohibits employment discrimination on the basis of race, color, religion, sex, and national origin and offers compensatory and

[125] Beauvais, Knoppers, & Illes, *supra* note 74; see also Farahany, *supra* note 80.

[126] As a related note, 'dual-use' of neuroscience information for both military and civilian interest may also raise important ethical and regulatory challenges. In addition, the use of the information by malevolent actors, for example, in the context of organized criminality, terrorist organizations, and other state and nonstate actors would engender national and global security concerns (Michael N. Tennison & Jonathan D. Moreno, *Neuroscience, Ethics, and National Security: The State of the Art*, 10 PLoS Biol. e1001289 (2012); Marcello Ienca, Fabrice Jotterand, & Bernice S. Elger, *From Healthcare to Warfare and Reverse: How Should We Regulate Dual-Use Neurotechnology?*, 97 Neuroview 269 (2018)). Legislative discussions on prohibition of misuse of neuroscience information may include how to define the role and limits of the use of neuroscience information in national security.

[127] Genetic Information Nondiscrimination Act of 2008 (GINA) Pub. L. No. 110–233, 122 Stat. 881 (2008).

[128] *Id.* When noncompliance was due to reasonable cause and not to willful neglect, the penalty is capped at 10% of the aggregate amount paid or incurred by the plan sponsor during the preceding year for group health plans or $500,000.

[129] 42 U.S.C. §2000e-5 (2010).

[130] *Id.*

punitive damages, reasonable attorney's fees, and injunctive relief (eg reinstatement, hiring, and back pay) for aggrieved employees.[131,132] In addition, GINA specifically prevents employers from retaliating against employees for bringing a complaint or for assisting others in their complaints.[133]

However, since GINA's enactment, actual legal cases filed under the act have been scarce. This low volume of cases might be due to the fact that people remain unfamiliar with protection against genetic discrimination in GINA and other laws or that there is little predictive genetic information meaningful enough to be used in health insurance and employment settings.[134] It could also indicate that discriminatory treatment is not pervasive in these settings.[135] From 2009 to 2018, there were no successful claims under the GINA filed in a federal court for discrimination based on genetic test results.[136] Chapman and colleagues also reported that the vast majority of GINA cases in employment settings are alleged violations of GINA's prohibition on requesting or requiring genetic information (eg illegal requests for information about family history of disease) rather than violations of its antidiscrimination provisions.[137] Relatedly, there has been 'no tsunami of efforts to reidentify people from their DNA or genomic data'.[138] It is likely this is because strong incentives exist to ensure confidentiality of genetic data, at least in the research and healthcare institution context, given potential federal and state penalties that could substantially limit research and clinical practices.[139] Moreover, given that other types of personal information, such as demographic and geographic information, can be more easily identifiable than genetic information can be, it is not clear how likely an attacker would seek to reidentify DNA to learn about an individual's genetic traits or propensities.[140]

It is important to keep in mind that the primary aim of GINA was not to redress ongoing or anticipated genetic discrimination but to 'allay [the public's] concerns about the potential for discrimination'.[141] In other words, GINA was enacted to assure people that participating in a genetic research study or undergoing genetic testing would not adversely affect them and thereby promote advances in genetic research and clinical care. A recent survey reported that about 13 per cent of patient respondents still expressed concerns about potential genetic discrimination in health insurance and the workplace when determining whether to enroll in genetic studies,[142] which reaffirms

[131] 29 C.F.R. § 1635.10(b) (2017), 75 Federal Register 68938 (November 9, 2012), referring to 42 U.S.C. § § 1981a(a)(1), (b); 1988(b), (c); 2000e-5(q).

[132] For employees covered by the Government Employee Rights Act of 1991, the Congressional Accountability Act of 1995, chapter 5 of Title 3 of the US Code, or Section 717 of the Civil Rights Act of 1964, the remedies and procedures contained in these Acts and statutory provisions apply.

[133] 42 U.S.C. §2000ff-6(f) (2008).

[134] Joly et al., *supra* note 79.

[135] *Id.*

[136] Bradley A. Areheart & Jessica L. Roberts, *GINA, Big Data, and the Future of Employee Privacy*, 128 Yale L. J. 710 (2019).

[137] Chapman et al., *supra* note 73.

[138] Clayton et al., *supra* note 77, at 27.

[139] *Id.*

[140] *Id.*

[141] 122 Stat. 881 §2(5) (2008).

[142] Laura M. Amendola et al., *Why Patients Decline Genomic Sequencing Studies: Experiences from the CSER Consortium*, 27 J. Genet. Couns. 1220 (2018).

the need for GINA's protection, even if it functions as a symbolic law, at least until to date.

The enforcement mechanism of GINA would provide a useful reference for the new legislation prohibiting misuse of neuroscience data. For example, in the context of health insurance, it might be necessary to refer to penalties for noncompliance with GINA in stipulating sanctions under the new legislation to ensure equitable enforcement against discrimination in health insurance. Yet, in legislative discussions, we would also want to consider the criticism concerning the effectiveness of the penalties under GINA, given the potentially expensive healthcare costs that may make violating the law more cost effective for health plans and health insurance issuers.[143] Similarly, as in GINA, remedies in Title VII of the Civil Rights Act of 1964 may also be extended to employment discrimination on the basis of neuroscience information, along with GINA's prohibition against retaliation.

Although it is critical to prescribe an effective enforcement mechanism that has the teeth in terms of accountability and penalties for violation, it is likely that the value of the new legislation prohibiting misuse of neuroscience information would, at least initially, be largely symbolic or expressive as in the case of GINA. As discussed above, there is a lack of empirical evidence substantiating the imminence of privacy concerns around neuroscience data. Decoding cognitive and affective states or predicting future outcomes from neuroscience data currently is at an exploratory stage and probably will remain so in the foreseeable future. Furthermore, it is currently impossible to obtain neuroscience data incidentally, compared with genetic information, which can be easily obtained without the individual's knowledge. In addition, no reports have been made about discrimination on the basis of neuroscience information or even reidentification of neuroscience data with malicious intent.

Nevertheless, extensive sensational media coverage on novel breakthroughs in neuroscience research has sparked popular interest in neuroscience research while simultaneously creating a fear of interference with our brains and a misuse of intimate information derived from neuroscience data. It was not specifically targeted to the public's attitude toward discrimination or unfavorable treatment on the basis of neuroscience information, but MacDuffie and colleagues' survey study showed substantial concerns around the issue of privacy regarding the collection of data on brain functioning using neural devices (eg fMRI, implanted brain or spinal stimulators, EEG, ultrasound, BCIs) and stigma due to the publicly visible features of a neural device (eg an electrode cap worn on the head) implicating a neurologic condition or illness.[144] Previous scholarly discussions on neuroscience data, which were often based on anticipatory projection as to what we can infer from neuroscience data, have also contributed to some hype around the privacy risk associated with the data; these discussions have also led to overly cautious regulatory solutions that could hinder beneficial use of neuroscience information.[145]

[143] Erwin, *supra* note 76.

[144] Katherine E. MacDuffie, Scott Ransom, & Eran Klein, *Neuroethics Inside and Out: A Comparative Survey of Neural Device Industry Representatives and the General Public on Ethical Issues and Principles in Neurotechnology*, 13 AJOB Neurosci. 44 (2021).

[145] Anna Wexler, *The Urgent Need to Better Integrate Neuroscience and Neuroethics*, 11 AJOB Neurosci. 219 (2020); Winston Chiong, *Insiders and Outsiders: Lessons for Neuroethics from the History of Bioethics*, 11

The new legislation would play a critical role in alleviating the fear of discriminatory or informational harm associated with neuroscience information and preventing harms in actual cases wherein unwanted or illicit disclosure of the information occurs, without sacrificing the benefits of scientific advancement using neuroscience information. Such legislation would also ensure that individuals would not be coerced to disclose their neuroscience information or subjected to unwanted collection of the information. Given the current premature state of technology, the new legislation might in fact operate as a safeguard against the abuse of unreliable inferences drawn from neuroscience data, as it would help protect against malicious use of neuroscience information regardless of the information's accuracy or credibility.

VI. CONCLUSION

The increase in the speed and scale of the collection and analysis of neuroscience data accompanied with advances in AI and big data analytics has spurred discussions about the need for heightened protection for neuroscience data. Researchers have argued that their uniquely sensitive nature and supposed potential to decode mental states and predict future outcomes make the privacy risk of neuroscience data particularly concerning compared with that of other personal data. Despite the current premature state of technology, a number of regulatory and policy approaches have been proposed out of an abundance of caution, primarily arguing for rigorous control of the collection, processing, and sharing of neuroscience data. Such approaches would enhance the protection of neuroscience data, but, at the same time, may impose a substantial burden on conducting neuroscience research and thus result in limiting the societal benefits of using neuroscience data. In addition, even with the best available privacy and security measures, it would be impossible to completely eliminate the risks of reidentification and unwanted disclosure of neuroscience data. Furthermore, disclosure of the data per se would hardly incur harm to subjects unless an actor with a malicious intent uses sensitive information within the data against subjects. In this article, we argued that there is a need to shift our attention from protecting neuroscience data to preventing potential harm from the malicious use of the data. We propose that developing a legal prohibition against misuse of information derived from neuroscience data, *Neuroscience Information Nondiscrimination Act*, could provide the ultimate protection against privacy risks of neuroscience data, as it would prevent harm associated with the data from occurring without unduly limiting open science practice for advances in neuroscience. Taking GINA as a reference, we examined some of the core questions needing to be addressed in developing this new legislation. These include why we would need a new regulatory protection specific to neuroscience information, why extending existing laws and regulations would not provide adequate protection against the misuse of information, how the term 'neuroscience information' should be defined under this new protection, in what contexts misuse of neuroscience information should be prohibited, and what the potential real-world impacts of this protection would be. We believe that this analysis would provide a useful foundation from which begin future regulatory discussion on governance of neuroscience data beyond data protection.

AJOB Neurosci. 155 (2020); Anna Wexler & Laura Specker Sullivan, *Translational Neuroethics: A Vision for a More Integrated, Inclusive, and Impactful Field*, AJOB Neurosci. (2021).

ACKNOWLEDGEMENTS

The authors thank Professor Henry T. Greely at Stanford Law School and Professor Nicole Martinez-Martin at Stanford Center for Biomedical Ethics for their valuable and constructive suggestions on earlier drafts of this article.

FUNDING

This article was fully funded by the National Institute of Mental Health (NIMH) grant number 3R24MH117179–04S1.

CONFLICT OF INTEREST

The authors declare no potential conflict of interest.