ARE YOU OUT OF YOUR MIND?: NEUROTECHNOLOGIES AND THE MAKING OF DISEMBODIED AGENCY

Daniel Levin†

> "Human beings are always already immersed in the world, in producing what it means to be human in relationships with each other and with objects . . . . If you start talking to people about how they cook their dinner or what kind of language they use to describe trouble in a marriage, you're very likely to get notions of tape loops, communication breakdown, noise and signal."
>
> —Donna Haraway[1]

> "We do not contemplate ourselves, but we exist only in contemplating—that is to say, in contracting that from which we come."
>
> —Gilles Deleuze[2]

ABSTRACT

This Paper expounds on the legal and philosophical implications underlying the development of brain-computer interfaces (BCIs). As it stands, the current U.S. legal regime is ill-equipped to redress emergent privacy harms in these BCI developments. By privileging identifiability through discrete data points and limited interpersonal contexts, these laws misapprehend how companies facilitate classification and identification through the construction of behavioral profiles constituted through psychographics and the combination of various data points with other contextual data. Privacy law's failure to appreciate the social

---

DOI: https://doi.org/10.15779/Z382Z12Q7D

† J.D., 2022, Fordham Law School. Daniel Levin is a Fellow at ZwillGen PLLC, assisting clients navigate compliance with U.S. and international data privacy frameworks applicable to emerging technologies. The Author would like to thank Professors Catherine Powell and Ari Waldman for developing this Paper throughout their seminar, Civil Rights and Civil Liberties in the Digital Age. The Author would also like to thank the editors at the Berkeley Technology Law Journal, who have offered invaluable suggestions and brought this Paper to print.

1. Hari Kunzru, *You Are Cyborg*, WIRED (Feb. 1, 1997), https://www.wired.com/1997/02/ffharaway/.

2. GILLES DELEUZE, DIFFERENCE AND REPETITION 74 (Paul Patton trans., Columbia Univ. Press 1994).

construction of doing privacy is by no means a sheer coincidence. Rather, it traces a genealogy to its normative underpinnings, wherein tech companies have "habituated us into thinking that managing our privacy is an individual responsibility."[3] In turn, our legal infrastructure entrenches a longstanding fallacy where privacy means control.

This Note considers these issues in four parts. Part II provides an overview of how BCIs developed through medical and scientific research, generating the preconditions for illicit use in employment, military, education, and consumer product contexts. Part III draws out the implications for neural data extraction and manipulation, focusing attention towards neuroethical and privacy considerations for emerging disembodied agency.[4] Part IV surveys deficiencies in existing privacy legal infrastructures for protecting neural data and, specifically, interrogates the underlying tenets to doing privacy law. Part V proposes a regulatory framework for protecting neural data that incorporates ongoing multi-stakeholder engagement to ensure that privacy law keeps pace with BCI's rapid innovation.

TABLE OF CONTENTS

I. INTRODUCTION

Over the past decade, technology companies have sought advancements in neurotechnology—especially in brain-computer interfaces (BCIs)—to perform behavioral analytics at more granular and exacting levels. Using electrical neural data, these systems decode responses to external stimuli and, in some instances, translate thought into rudimentary speech or muscle movements. While these uses are integral to enabling autonomy for disabled persons, their expanding use in workplace and consumer settings risk

3. Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 CALIF. L. REV. 1221, 1227 (2022).

4. This Note uses the term "disembodied agency" to refer to the ability to act without using the body to mediate such action. Whereas an agent typically "thinks before acting," BCIs risk converging the space between thought and action, producing agents that think and act simultaneously, and render thought itself into action.

undermining the distance users need to process stimuli beyond mere intuitions and to narrate their responses to such stimuli. At the same time, the privacy risks endemic to these technologies remain constant among their users, with more disproportionate effects burdening disabled communities.

Such recent advances in neurotechnology risk displacing users' sense of personhood. With the advent of BCIs—or, the use of machine learning technologies to decode neural data and elicit speech or motor responses—the gap between human and machine shrinks. As these technologies integrate the brain with external devices, balancing their medical benefits with their ethical and privacy implications becomes increasingly complex., BCIs assimilate neurodivergent persons into "normalcy," eroding their privacy to "think for themselves."[5] This highlights an underlying tenet to privacy scholarship: privacy enables the precondition for thinking, such that meaningful expression becomes possible. Neil Richards popularized this phenomenon as "intellectual privacy," arguing that "[t]he ability to freely make up our minds and to develop new ideas . . . depends upon a substantial measure of intellectual privacy."[6]

Indeed, just as privacy provides the precondition for thinking, thinking provides the precondition for being. Making sense of our interactions requires the space to reflect on the transition from intention and emotion to expression. While useful in limited medical and rehabilitative contexts—such as enabling para- and tetraplegic persons to elicit muscle movements[7] or think language into external speech[8]—the expansion of BCI-enabled capacities could erode this reflection process. Nevertheless, we should be wary of technologists' half-

5. Eran Klein, Sara Goering, Josh Gagne, Conor V. Shea, Rachel Franklin, Samuel Zorowitz, Darin D. Dougherty & Alik S. Widge, *Brain-Computer Interface-Based Control of Closed-Loop Brain Stimulation: Attitudes and Ethical Considerations*, 3 BRAIN-COMPUT. INTERFACES 140, 140 (2016).

6. Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 389 (2008).

7. *See, e.g.*, Samuel C. Colachis IV, Marcie A. Bockbrader, Mingming Zhang, David A. Friedenberg, Nicholas V. Annetta, Michael A. Schwemmer, Nicholas D. Skomrock, Walter J. Mysiw, Ali R. Rezai, Herbert S. Bresler & Gaurav Sharma, *Dexterous Control of Seven Functional Hand Movements Using Cortically-Controlled Transcutaneous Muscle Stimulation in a Person With Tetraplegia*, 12 FRONTIERS NEUROSCI. 1, 1 (Apr. 4, 2018), https://doi.org/10.3389/fnins.2018.00208.

8. *See, e.g.*, Robin Marks, *"Neuroprosthesis" Restores Words to Man with Paralysis*, U. CAL. S.F. (July 14, 2021), https://www.ucsf.edu/news/2021/07/420946/neuroprosthesis-restores-words-man-paralysis.

truths, mischaracterizing BCIs' "mind-reading" [9] or "skill-uploading" [10] capacities. But sobering ourselves to the current state of the technology should not dissuade us from considering whether to reorient its development.

As it stands, the current U.S. legal regime is ill-equipped to redress emergent privacy harms in these BCI developments. By privileging identifiability through discrete data points and limited interpersonal contexts, these laws misapprehend how companies facilitate classification and identification through the construction of behavioral profiles constituted through psychographics and the combination of various data points with other contextual data. Privacy law's failure to appreciate the social construction of doing privacy is by no means a sheer coincidence. Rather, it traces a genealogy to its normative underpinnings, wherein tech companies have "habituated us into thinking that managing our privacy is an individual responsibility."[11] In turn, our legal infrastructure entrenches a longstanding fallacy where privacy means control.

This Note considers these issues in four parts. Part II provides an overview of how BCIs developed through medical and scientific research, generating the preconditions for illicit use in employment, military, education, and consumer product contexts. Part III draws out the implications for neural data extraction and manipulation, focusing attention towards neuroethical and privacy considerations for emerging disembodied agency. [12] Part IV surveys deficiencies in existing privacy legal infrastructures for protecting neural data and, specifically, interrogates the underlying tenets to doing privacy law. Part V proposes a regulatory framework for protecting neural data that incorporates ongoing multi-stakeholder engagement to ensure that privacy law keeps pace with BCI's rapid innovation.

II. WHAT ARE BCIS?

Any attention to privacy and ethical concerns endemic to technologies must first grapple with how the technology works. As a preliminary matter,

9. Josh Constine, *Facebook is Building Brain-Computer Interfaces for Typing and Skin-hearing*, TECHCRUNCH (Apr. 19, 2017), https://techcrunch.com/2017/04/19/facebook-brain-interface/.

10. Daniel Kolitz, *Will It Be Possible to Upload Information to My Brain?*, GIZMODO (Sept. 20, 2021), https://gizmodo.com/will-it-be-possible-to-upload-information-to-my-brain-1847698784.

11. Waldman, *supra* note 3, at 1227.

12. This Note uses the term "disembodied agency" to refer to the ability to act without using the body to mediate such action. Whereas an agent typically "thinks before acting," BCIs risk converging the space between thought and action, producing agents that think and act simultaneously, and render thought itself into action.

this Part seeks to categorize BCIs' primary types and user inputs, providing examples when applicable of how these devices extract, transform, and respond to user information. This Part also details a brief overview of BCI development and provides various use cases to demonstrate its growing traction beyond traditional medical rehabilitation.

A. Categorizing BCI Types and User Inputs

Today's BCIs fall broadly into one of two types: invasive or non-invasive. As the name suggests, invasive BCIs refer to implants installed directly into or on top of the user's brain. Such devices require surgical procedure to install the device. Typically, these BCIs only appear in medical contexts. The second type—non-invasive BCIs—use external electrodes or other sensors connected to the body for collecting and modulating neural signals. Whereas the former appears mostly in medical contexts, the latter holds more traction among both medical and consumer products, typically appearing as wearable headbands and wristbands.

While researchers tend to divide BCIs into these two types, it bears mentioning that the term "non-invasive" serves as a misnomer. To the extent that these devices may still register neural data and stimulate users accordingly, they produce similar effects to their "invasive" counterparts, namely modulating neural activity. For example, transcranial direct current stimulation (TDCS) direct electrical currents to specific parts of the brain to enhance users' memory retention and learning capabilities.[13] Additionally, electromyography (EMG) sensors attach to users' wrists and may record motor neurons and muscular electrical activity.[14] Currently, these devices aid in diagnosing neuromuscular abnormalities, though researchers have garnered interest in integrating EMG to detect users' intent to move their fingers for operating virtual keyboards and external devices.[15] By reducing the calculus to BCIs' surgical component, researchers developed an arbitrary division between "invasive" and "non-invasive" BCIs, which mischaracterizes the technology's fundamental nature in modulating neural activity.

13. *See* Nicola Riccardo Polizzotto, Nithya Ramakrishnan & Raymond Y. Cho, *Is It Possible to Improve Working Memory with Prefrontal tDCS? Bridging Currents to Working Memory Models*, 11 FRONTIERS PSYCH. 1, 1 (2020), https://www.frontiersin.org/articles/10.3389/fpsyg.2020.00939/full.

14. *See* Adi Robertson, *I Tried the Wristband that Lets You Control Computers with Your Brain*, VERGE (Jun. 6, 2018), https://www.theverge.com/2018/6/6/17433516/ctrl-labs-brain-computer-interface-armband-hands-on-preview.

15. Reality Lab, *Inside Facebook Reality Labs: The Next Era of Human-Computer Interaction*, FACEBOOK (Mar. 8, 2021), https://tech.facebook.com/reality-labs/2021/3/inside-facebook-reality-labs-the-next-era-of-human-computer-interaction/.

Once researchers develop either an invasive or non-invasive device, they distinguish user inputs through two primary categories. First, with active BCIs, users intentionally perform mental tasks that produce designated patterns of brain activity.[16] Typically, this involves capturing neural signals that imagine moving the body or eliciting some act. These signals derive from motor cortical areas of the brain, such that we can activate movements merely through *intending* such movements.[17] As this Note discusses below, closing the gap between intention and action may incur dire consequences for users' ability to exercise agency and autonomy, disabling the necessary space to think before acting. While these effects are generalizable, these technologies disproportionately displace these harms onto disabled users, who lack sufficient recourse to opt out. Indeed, to the extent that such technologies mediate action through intention, they also turn intentions *into* actions.

Second—in opposition to active BCIs—passive BCIs monitor brain activity to detect patterns.[18] These have been integral to generating affective computing systems that recognize lapses in emotional state and attention, such that employers can predict and preempt dangerous workplace situations.[19] For example, these passive BCIs may detect "unintentional changes in a user's cognitive state as an input for other adaptive systems," such that detection of a driver's drowsiness may prompt their vehicle to either change the temperature or the volume of the sound system to increase the driver's alertness.[20] They also show promise in predicting cognitive and affective states for modulating (and sometimes improving) user-adaptive interaction.[21] For

16. *See* Steffen Steinert, Christoph Bublitz, Ralf Jox & Orsolya Friedrich, *Doing Things with Thoughts: Brain-Computer Interfaces and Disembodied Agency*, 32 PHIL. & TECH. 457, 460 (2018).

17. For a few examples of these BCIs, see generally Ritik Looned, Jacob Webb, Zheng Gang Xiao & Carlo Menon, *Assisting Drinking With an Affordable BCI-Controlled Wearable Robot and Electrical Stimulation: A Preliminary Investigation*, 11 J. NEUROENG'G & REHAB. 51 (2014) (commanding neuroprosthetic arm to drink); Ferran Galán Marnix Nuttin, Eileen Lew, Pierre W. Ferrez, Gerolf Vanacker, Johan Philips & J. del R. Millán, *A Brain-Actuated Wheelchair: Asynchronous and Non-invasive Brain–Computer Interfaces for Continuous Control of Robots*, 119 CLINICAL NEUROPHYSIOLOGY 1 (2008) (using neural data to drive wheelchair); Serafeim Perdikis, Robert Leeb, John Williamson, Amy Ramsay, Michele Tavella, Lorenzo Desideri, Evert-Jan Hoogerwerf, Abdul Al-Khodairy, Roderick Murray-Smith & J. d R Millán, *Clinical Evaluation of BrainTree, A Motor Imagery Hybrid BCI Speller*, 11 J. NEURAL ENG'G 1 (2014) (controlling a spelling application).

18. *See* Steinert et al., *supra* note 16, at 461.

19. *See* Thorsten O. Zander & Christian Kothe, *Towards Passive Brain–Computer Interfaces: Applying Brain–Computer Interface Technology to Human–Machine Systems in General*, 8 J. NEURAL ENG'G 1, 2–4 (2011).

20. Maryam Alimardani & Kazuo Hiraki, *Passive Brain-Computer Interfaces for Enhanced Human-Robot Interaction*, 7 FRONTIERS ROBOTICS & AI 1, 2 (2020).

21. *See id.* at 1.

example, when users interface in gaming environments through BCIs, they may experience frustration or boredom, signaling that the game should either decrease its level of difficulty or, alternatively, introduce additional elements for engagement.[22]

B. Expanding Applications for BCIs

At first relegated to rehabilitation, BCIs were integrated into medical environments to assist patients with debilitating illnesses. For example, patients with essential tremors and Parkinson's disease used BCIs to identify and stimulate curative brain activities.[23] Those with locked-in syndrome could elicit muscular movements and engage in rudimentary speech.[24] Recent advancements have converted paralyzed persons' thoughts into texts[25] and generated artificial vision for the blind.[26]

While the technology remains nascent, recent developments demonstrate its growing traction beyond medical use. In Barcelona, the Synthetic, Perceptive, Emotive and Cognitive Systems (SPECS) Group at the Institute for Bioengineering of Catalonia used an active BCI to conduct an orchestral performance through brain waves and heart rate alone.[27] Performers shifted their attention between varying visual frequencies, enunciating an emotional experience devoid of any bodily expression.[28] Other researchers demonstrated

---

22. *See* Christian Mühl, Brendan Allison, Anton Nijholt & Guillaume Chanel, *A Survey of Affective Brain Computer Interfaces: Principles, State-of-the-Art, and Challenges*, 1 BRAIN-COMPUT. INTERFACES 66, 68 (2014).

23. *Deep Brain Stimulation (DBS) for the Treatment of Parkinson's Disease and Other Movement Disorders*, NAT'L INST. NEUROLOGICAL DISORDERS & STROKE, https://web.archive.org/web/20220110115505/https://www.ninds.nih.gov/About-NINDS/Impact/NINDS-Contributions-Approved-Therapies/DBS.

24. Daniel Engber, *The Neurologist Who Hacked His Brain—And Almost Lost His Mind*, WIRED (Jan. 26, 2016), https://www.wired.com/2016/01/phil-kennedy-mind-control-computer/.

25. Peter Dockrill, *Brain Implant Translates Paralyzed Man's Thoughts Into Text With 94% Accuracy*, SCI. ALERT (Nov. 8, 2021), https://www.sciencealert.com/brain-implant-enables-paralyzed-man-to-communicate-thoughts-via-imaginary-handwriting.

26. Carly Cassella, *Brain Implant Gives Blind Woman Artificial Vision in Scientific First*, SCI. ALERT (Oct. 27, 2021), https://www.sciencealert.com/a-brain-implant-has-allowed-a-blind-woman-to-see-simple-2d-shapes-and-letters.

27. Jason Palmer, *World Premiere of Brain Orchestra*, BBC NEWS (Apr. 24, 2009), http://news.bbc.co.uk/2/hi/science/nature/8016869.stm.

28. *Id.*

success in manipulating external objects, including control of drone flight,[29] mobile devices,[30] and computer games.[31]

Yet these emerging uses stray from the technology's origins. Paralleling developments for medical use, researchers have sought to refine existing non-medical uses across various applications. Over the last decade alone, researchers have applied BCIs to lie detection,[32] detecting drowsiness for human work performance,[33] estimating reaction times,[34] and controlling virtual reality environments.[35]

---

29. Karl LaFleur, Kaitlin Cassady, Alexander Doud, Kaleb Shades, Eitan Rogin & Bin He, *Quadcopter Control in Three-Dimensional Space Using a Noninvasive Motor Imagery-based Brain–Computer Interface*, 10 J. NEURAL ENG'G 1, 3 (2013).

30. Susan Young Rojahn, *Samsung Demos a Tablet Controlled by Your Brain*, MIT TECH. REV. (Apr. 19, 2013), https://www.technologyreview.com/2013/04/19/253309/samsung-demos-a-tablet-controlled-by-your-brain/.

31. Minkyu Ahn, Mijin Lee, Jinyoung Choi & Sung Chan Jun, *A Review of Brain-Computer Interface Games and an Opinion Survey from Researchers, Developers and Users*, 14 SENSORS 14601, 14613 (2014).

32. Lawrence A. Farwell, Drew C. Richardson, Graham M. Richardson & John J. Furedy, *Brain Fingerprinting Classification Concealed Information Test Detects US Navy Military Medical Information with P300*, 8 FRONTIERS NEUROSCI. 1, 1 (2014).

33. *See* Pietro Aricò, Gianluca Borghini, Gianluca Di Flumeri, Alfredo Colosimo, Stefano Bonelli, Alessia Golfetti, Simone Pozzi, Jean-Paul Imbert, Géraud Granger, Raïlane Benhacene & Fabio Babiloni, *Adaptive Automation Triggered by EEG-Based Mental Workload Index: A Passive Brain-Computer Interface Application in Realistic Air Traffic Control Environment*, 10 FRONTIERS HUM. NEUROSCI. 1, 3 (2016); Chun-Shu Wei, Yu-Te Wang, Chin-Teng Lin & Tzyy-Ping Jung, *Toward Drowsiness Detection Using Non-hair-Bearing EEG-Based Brain-Computer Interfaces*, 26 IEEE TRANSACTIONS ON NEURAL SYS. & REHAB. ENG'G 400, 400 (2018)*; see also* Stephen Chen, *'Forget the Facebook Leak': China is mining data directly from workers' brains on an industrial scale*, S. CHINA MORNING POST (Apr. 29, 2018), https://www.scmp.com/news/china/society/article/2143899/forget-facebook-leak-china-mining-data-directly-workers-brains. *See generally* Xiaoliang Zhang, Jiali Li, Yugang Liu, Zutao Zhang, Zhuojun Wang, Dianyuan Luo, Xiang Zhou, Miankuan Zhu, Waleed Salman, Guangdi Hu & Chunbai Wang, *Design of a Fatigue Detection System for High-Speed Trains Based on Driver Vigilance Using a Wireless Wearable EEG*, 17 SENSORS 486 (2017) (describing a novel fatigue detection system for high-speed train safety based on monitoring train driver vigilance using a wireless wearable EEG).

34. *See generally* Dongrui Wu, Brent J. Lance, Vernon J. Lawhern, Stephen Gordon, Tzyy-Ping Jung & Chin-Teng Lin, *EEG-Based User Reaction Time Estimation Using Riemannian Geometry Features*, 25 IEEE TRANSACTIONS ON NEURAL SYS. & REHAB. ENG'G 2157 (2017) (validating the performance of a new proposed approach for EEG-based BCI regression problems in reaction time estimation from EEG signals measured in a large-scale sustained-attention psychomotor vigilance task).

35. *See generally* Athanasios Vourvopoulos, Octavio Marin Pardo, Stéphanie Lefebvre, Meghan Neureither, David Saldana, Esther Jahng & Sook-Lei Liew, *Effects of a Brain-Computer Interface With Virtual Reality (VR) Neurofeedback: A Pilot Study in Chronic Stroke Patients*, 13 FRONTIERS HUM. NEUROSCI. 1 (2019) (combining the principles of VR and BCI in a REINVENT platform to assess its effects on four chronic stroke patients across different levels of motor impairment).

Today, as the race ensues to build out an embodied internet through the "metaverse," companies hedge their bets on integrating BCI technologies—typically electroencephalogram (EEG) wearables—into immersive environments.[36] For example, in 2019, Meta acquired CTRL-Labs, a startup developing wristbands that use muscular electrical activity to control external devices.[37] Similarly, in 2022, Snap acquired NextMind, a startup developing headbands to perform comparable functions.[38] Both Meta and Snap expressed interest in deploying these devices in virtual and augmented reality settings.[39] With a growing enthusiasm for expanding BCI applications, researchers and developers are working to broaden human experiences through these settings, including the capacity to experience not only one's own feelings and sensations in these immersive environments, but also other users'.[40] All the while, there remain significant limitations in examining the privacy and ethical concerns in both the development and deployment of BCIs.

III. PRIVACY AND ETHICAL CONSIDERATIONS FOR DISEMBODIED AGENCY

Because BCIs' intended uses are heterogeneous, these technologies risk reproducing asymmetries in users' human experience. On one hand, those with disabilities require these advancements to assimilate into able-bodied society. On the other hand, those without disabilities may avail themselves of human experiences that transcend having a body. As this Note suggests, the privacy and ethical concerns endemic to both sets of users are the same: the technology displaces the body into a sequence of automatisms, reconfiguring how we understand an emerging disembodied agency that undermines the integrity of thought.

---

36. *See* Amir Reza Asadi, *BCI for Metaverse*, METAVERSE CHI (Mar. 24, 2022), https://metaverse.acm.org/bci-for-interaction-with-metaverse/; Sissi Cao, *Mark Zuckerberg Teases AI 'Brain Chip'—But It Will Be Different than Elon Musk's*, OBSERVER (Oct. 12, 2019), https://observer.com/2019/10/mark-zuckerberg-ai-brain-chip-elon-musk-neuralink/.

37. Nick Statt, *Facebook Acquires Neural Interface Startup CTRL-Labs for its Mind-Reading Wristband*, VERGE (Sept. 23, 2019), https://www.theverge.com/2019/9/23/20881032/facebook-ctrl-labs-acquisition-neural-interface-armband-ar-vr-deal.

38. Sissi Cao, *Snap's Latest Acquisition is a Bet on a Metaverse Controlled by Thoughts*, OBSERVER (Mar. 24, 2022), https://observer.com/2022/03/snap-acquire-nextmind-brain-computer-interface-metaverse/.

39. *Id.*; Cao, *supra* note 36.

40. Sergio López Bernal, Mario Quiles Pérez, Enrique Tomás Martínez Beltrán, Gregorio Martínez Pérez & Alberto Huertas Celdrán, *When Brain-Computer Interfaces Meet the Metaverse: Landscape, Demonstrator, Trends, Challenges, and Concerns*, ARXIV (Dec. 6, 2022), https://arxiv.org/pdf/2212.03169.pdf.

This Part details three chief privacy concerns, each building on each other. First, trends in BCI development intrude on data subjects' autonomy over their emotions and subject them to greater vulnerability to emotional manipulation.[41] Specifically, BCI development refines existing means for interpreting data subjects' affective states, registering emotion-related responses to external stimuli as a means for contextualizing and modulating users' disposition towards such stimuli.[42] Second, BCIs exacerbate general issues with machine learning technologies, wherein statistical inferences may potentially misidentify and entrench users' affective states. Third, by registering users' response to stimuli and modulating their neural activity accordingly, BCIs enter a feedback loop that divorces users from the deliberative process to reflect on their own thoughts and instantiate some act upon their own volition.

As later-discussed developments in BCIs indicate, the technology trends towards intruding on data subjects' autonomy over their emotions. Specifically, BCI development traces a genealogy of using technology to interpret and modulate data subjects' affective states. With the current state of neural imaging, discrete neural data points have little capacity to identify their users, let alone any particular ailments they suffer.[43] But such identifications—or differentiations, as the literature describes—have proven possible through the collection of 30-second recordings of brain activity.[44] Through neural fingerprinting, BCIs generate inferences about individual biology and cognitive states, rendering information about users' moods, intentions, and physiological characteristics.[45] These reverse inferences register patterns of brain activity to approximate specific cognitive states.[46] Thus, while they do not decode thoughts—as in, translate granular accounts of neural patterns into specific cognitive processes—they provide an exacting mechanism for processing perceptions to stimuli and subjecting them to manipulation.

41. *See generally* Steffen Steinert & Orsolya Friedrich, *Wired Emotions: Ethical Issues of Affective Brain-Computer Interfaces*, 26 SCI. & ENG'G ETHICS 351 (2020) (providing an overview of ethical issues with BCIs that allow for the detection and stimulation of affective states).

42. *Id.* at 352.

43. Jeremy Greenberg, Katelyn Ringrose, Sara Berger, Jamie VanDodick, Francesca Rossi & Joshua New, *Privacy and the Connected Mind*, FUTURE PRIV. F. (Nov. 2021), https://fpf.org/wp-content/uploads/2021/11/FPF-BCI-Report-Final.pdf.

44. Jason da Silva Castanheira, Hector Domingo Orozco Perez, Bratislav Misic & Sylvain Baillet, *Brief Segments of Neurophysiological Activity Enable Individual Differentiation*, 12 NATURE COMMC'NS. 1, 2 (2021).

45. Greenberg et al., *supra* note 43, at 9.

46. Russell A. Poldrack, *Inferring Mental States from Neuroimaging Data: From Reverse Inference to Large-Scale Decoding*, 72 NEURON 692, 697 (2011).

Just as BCI developments may be situated within a broader trajectory to interpret and modulate data subjects' affective states, they suffer from the same limitations of other machine learning technologies. Using predictive algorithms, these data analyses provide more than passive determinations; they provoke certain responses that divorce users from contexts that otherwise elicit human decisional conflicts in the first place. Put differently, efforts to refine behavioral analytics result in pitching contexts that ensure specific behavioral responses, with increasing precision relative to the granularity of data collected.

For example, BCIs may deduce erroneous patterns in behavior and, in turn, register such deductions for predictive purposes. To illustrate this, an individual operating a neuroprosthetic—such as a BCI-controlled wheelchair or arm—may experience hunger and intend movement towards a particular food item in sight. While the event occurred through a confluence of circumstances, the BCI would register extraneous information that may otherwise prove irrelevant, such as when and where the user experienced hunger and what item induced such feelings or intentions. Devoid of context, these neural patterns train the device to ascertain specific preferences. Consequently, BCIs may usurp users' decision-making capacity to the extent that they have registered historical data about users' past decisions as proxies for their future decisions. For example, a user may operate a BCI-controlled wheelchair that not only deduces that the user is thinking about food, but also registers inferences about the user's biology and preferences around whether a user is hungry and the times.[47] To this extent, these devices may limit the possibility for users to meaningfully exercise autonomy over future decisions and make significant departures from such past decisions. This problem recapitulates what Kate Crawford critiqued of machine learning technologies generally, namely that "machine learning exploits what it does know to predict what it does not know: a game of repeated approximations."[48]

Beyond these deductions, BCIs may relate neural data to other contextual indicia, drawing disparate statistical inferences on otherwise irrelevant data points. Assumed to magnify the context, BCIs may integrate neural data with voice recordings, smartphone, social media usage data, and geolocation to signify greater meaning to neural activity.[49] The practice of relating these data

47. Greenberg et al., *supra* note 43, at 13.

48. KATE CRAWFORD, THE ATLAS OF AI: POWER, POLITICS, AND THE PLANETARY COSTS OF ARTIFICIAL INTELLIGENCE 221 (2021).

49. Marcello Ienca, Joseph J. Fins, Ralf J. Jox, Fabrice Jotterand, Silja Voeneky, Roberto Andorno, Tonio Ball, Claude Castelluccia, Ricardo Chavarriaga, Hervé Chneiweiss, Agata Ferretti, Orsolya Friedrich, Samia Hurst, Grischa Merkel, Fruzsina Molnár-Gábor, Jean-Marc

points to identify users' interests corresponds to what Brittan Heller has termed "biometric psychography."[50]

Under this calculus, biometric psychography positions behavioral and anatomical information—such as pupil dilation—to measure users' reactions to stimuli over time.[51] As Heller wrote, this can reveal not only users' physical, mental, and emotional states, but also the stimuli causing the user to enter that state.[52] Rather than using that data to achieve identification, these technologies produce broader inferences about users' values and attitudes, and can incorporate such inferences into more refined neuromarketing schemes.[53]

By situating BCIs within a broader trajectory to interpret data subjects, stakeholders can understand how privacy over neural data provides the prerequisite for self-realization and community-building. Mental privacy enables us to regulate the interpersonal and spatial interactions that constitute identity.[54] Disrupting that cognitive control affects the very process for identity-formation and ruptures the distance to engage in self-reflection. With BCIs, the distance that mediates such regulation closes, coercing users to engage in suppressing thoughts that may otherwise be integral to informing their values and, eventually, their actions.

Relying on historical data to render future decisions, BCIs enter a feedback loop that divorces users from deliberating and thinking before acting, limiting the scope of potential actions that may otherwise result from that deliberative process. Put otherwise, as intention itself *becomes* action, the ability to exercise executory control shrinks, thereby preempting the ability to think about our thoughts without automatically instantiating them. Rather than acting upon volition, BCI technologies encourage users to increasingly act without a conscious apprehension of a given moment, sublimating action into a sequence of instincts. Picking up on the underlying signal, BCIs translate thoughts into movements and render meaning to such thoughts that, in turn, inform further action. These actions devolve into automatisms, reflexively habituating thought into intuitions.

Rickli, James Scheibner, Effy Vayena, Rafael Yuste & Philipp Kellmeyer, *Towards a Governance Framework for Brain Data*, 15 NEUROETHICS 1, 3 (2022).

50. Brittan Heller, *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law*, 23 VAND. J. ENT. & TECH. L. 1, 27 (2021).

51. *Id.*

52. *Id.*

53. Marcello Ienca, Pim Haselager & Ezekiel J. Emanuel, *Brain Leaks and Consumer Neurotechnology*, 36 NATURE BIOTECH. 805, 805–10 (2018).

54. Abel Wajnerman Paz, *Is Mental Privacy a Component of Personal Identity?*, 15 FRONTIERS HUM. NEUROSCI. (Oct. 2021); *see also* Julie Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1905 (2013).

Such inferential power facilitates more exacting disclosures of mental information.[55] Because BCIs retain the capacity to read and modulate brain activity, they pose a significant threat to manipulative stimulation at unprecedented scale. Additionally, these technologies enable covert forms of discrimination predicated on neural signatures, including mental health, personality traits, cognitive performance, intentions, and emotional states.[56] Such signatures are fed into automated systems that could draw statistical inferences about group character and behavior, presupposing some inherence in responses to stimuli or a predisposition to certain cognitive processes.[57] For example, processing neural data may indicate a predisposition to dementia or prodromal cognitive decline, which could result in data controllers' access to (and potential disclosure of) sensitive information about these users.[58]

Research has demonstrated such interest in deploying machine learning techniques to read brain states and predict users' movement intentions, bypassing the deliberative process for users to provide commands.[59] But neural data does little to explain users' inner machinations, let alone the historical forces that habituate and inform such deliberative processes. Indeed, they divorce users from reflection, potentiating a host of vulnerabilities that may include embarrassing disclosures—including about one's sexuality or gender—or outright violent acts.

Yet the current research seldom addresses and has undertheorized these privacy concerns. By focusing predominantly on the technology's intended uses and effects, the overwhelming bulk of scientific literature, in particular, escapes meaningful discourse on BCIs' privacy and ethical harms. As developers trend towards privacy and accessibility by design, these contributions will prove critical to producing more equitable technologies in use and kind.

Privacy scholarship on BCIs has begun to fill in these gaps, though it remains sparse. Among the scholarship, authors have challenged how neural

---

55. Ienca et al., *supra* note 49, at 5.

56. *Id.* at 7.

57. *Id.* at 8. These practices risk reproducing now-defunct racist pseudo-sciences—such as physiognomy and phrenology—which conform certain external manifestations of expression into legible mental faculties. Though beyond the scope of this Note, I argue that the process of translating neural signals into neural data generates a similar external manifestation that renders analyses devoid of context. *See generally* Luke Stark & Jevan Hutson, *Physiognomic Artificial Intelligence*, 32 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 922 (2022) (discussing reanimation of pseudosciences in emerging technologies).

58. Ienca et al., *supra* note 49, at 7, 9.

59. Yijun Wang & Tzyy-Ping Jung, *A Collaborative Brain-Computer Interface for Improving Human Performance*, 6 PLOS ONE 1, 1 (2011), https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0020422.

engineering poses new concerns to the Fifth Amendment's self-incrimination doctrine, blurring the traditional distinction between testimonial and physical evidence.[60] Others have identified the technical and security vulnerabilities that such devices have, rendering BCIs susceptible to adversarial attacks and leaving users at risk of mental and physical manipulation.[61] In these instances, "brain malware" may extract users' neural data by either "hijacking the legitimate components of a BCI system" or "adding or replacing the legitimate BCI components."[62] These contributions have been integral to informing the theoretical backdrop for BCIs, though the works seldom consider how BCIs' data practices incur privacy harms, let alone how they interact with privacy law.

IV. STRUCTURAL FAILURES IN AND OF PRIVACY LAW

In light of their ability to convert intentions into actions, BCIs threaten core foundations that constitute personhood. By reducing thought into quantifiable metrics, the technology removes thought from the province of our minds, thereby limiting the possibility to engage in alternative actions beyond the device's registered data. Moreover, they contribute to a growing political economy that adheres to an "extraction imperative," borne out of profit-driven motivations to predict something "essential" to our person.[63]

Indeed, for those made reliant on the technology—especially those among disabled communities—these risks imperil users' ability to narrate and realize themselves on their terms. In light of these risks, privacy law offers little recourse for protecting neural data from companies' encroachment. Existing law entrenches a banal view of *doing* privacy, reducing it to procedural checklists like performing diligence and conducting impact assessments. In turn, privacy professionals further a culture that serves corporate interests under the guise of advancing privacy, performing tasks given to them within a constraining organization.[64] As this Part lays out, privacy law therefore suffers from structural deficiencies, many of which are irremediable without overhauling predominating discourses around *doing* privacy.

Accordingly, this Part details three key failures in federal and state privacy laws alike. First, sectoral privacy laws place too much emphasis on the types of relationships mediating information flows, rather than the information

60. Nita Farahany, *Incriminating Thoughts*, 64 STAN. L. REV. 351, 394–400 (2012).

61. Tamara Bonaci, Ryan Calo & Howard Jay Chizeck, *App Stores for the Brain: Privacy & Security in Brain-Computer Interfaces*, IEEE TECH. & SOC'Y MAG. 35–39 (June 2015).

62. *Id.* at 35.

63. SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 87 (2019).

64. Waldman, *supra* note 11, at 1268–69.

itself. Second, because privacy laws tend to follow consequentially to innovation, their definitions of phenomena are often too narrow in scope to capture new ways of understanding (and regulating) such phenomena, as exemplified in biometric privacy laws. Third, because companies rely on such narrow definitions to comply with existing law, they simultaneously inform how regulators and standard-setting organizations understand compliance themselves, in turn deferring to corporate norms to govern privacy.

In its current iteration, privacy law remains a fragmented regime that privileges disparate interests in information relative to particular relationships. For example, health privacy laws, like the Health Insurance Portability and Accountability Act (HIPAA), narrowly govern the doctor-patient relationship.[65] Because HIPAA was enacted prior to our burgeoning landscape of consumer medical technologies, these technologies evade scrutiny and enable corporate actors to operate outside of HIPAA's purview, all the while extracting the same information.[66] Companies' outlandish claims to "access and absorb knowledge instantly from the cloud or . . . pump images from one person's retina straight into the visual cortex of another"[67] run amok, enabled through a neoliberal legal apparatus that recapitulates what Julie Cohen termed the "surveillance-innovation complex."[68]

Additionally, privacy law reproduces limited understandings of phenomena, narrowly drafting definitions that should otherwise qualify as personal information. For example, biometric privacy laws privilege recognition through external physiological features.[69] Newer legislation has expanded understandings of biometrics to "behavioral characteristics," but then exemplifies biometric information through imagery of retinas,

---

65. *HIPAA: Covered Entities and Business Associates*, U.S. DEP'T HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (last visited Apr. 11, 2023).

66. *Concerns Raised About the Sharing of Health Data with Non-HIPAA Covered Entities via Apps and Consumer Devices*, HIPAA J. (Mar. 27, 2019), https://www.hipaajournal.com/concern-sharing-health-data-non-hipaa-covered-entities/.

67. *How Brains and Machines Can be Made to Work Together*, ECONOMIST (Jan. 4, 2018), https://www.economist.com/technology-quarterly/2018/01/04/how-brains-and-machines-can-be-made-to-work-together.

68. JULIE COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 89 (2019).

69. *See, e.g.*, 740 ILL. COMP. STAT. 14/10 (2008) ("'Biometric identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.").

fingerprints, and facial geometries.[70] And, unless neural data alone can identify an individual, it evades legal definitions for personal information.[71]

Such biometric laws are not only deficient in defining "biometrics," but also in their scope of protection.[72] Currently, only Illinois,[73] Texas,[74] and Washington[75] have enacted specific biometric privacy laws, with Illinois serving as the only state among them to provide consumers with a private right of action. In California, the state's omnibus privacy statute only provides a private right of action where the biometric information was subject to an unauthorized exposure resulting from a business's failure to implement and maintain reasonable security procedures.[76]

As it stands, no single law—neither federal nor state—governs data practices relating to neural data. By consequence, companies escape liability and remain compliant to the extent that their innovations escape existing laws' structural deficiencies to adequately define and protect this information. Absent these substantive protections to guide the development and implementation of these technologies, companies could leverage neural data as a commodity to produce consumer neurotechnologies, e-learning, digital phenotyping, affective computing, psychographics, and neuromarketing.[77]

Indeed, these deficits in legal protection enable companies to engage in privacy intrusions with relative impunity. As Daniel Solove and Woodrow Hartzog argue, existing enforcement bodies—such as the Federal Trade Commission (FTC)—defer to corporate privacy norms.[78] Specifically, the

70. CAL. CIV. CODE § 1798.140(b) (2021).

71. *See, e.g.*, *California Consumer Privacy Act (CCPA)*, ATT'Y GEN. ROB BONTA, https://oag.ca.gov/privacy/ccpa ("Personal information is information that identifies, relates to, or could reasonably be linked with you or your household. For example, it could include your name, social security number, email address, records of products purchased, internet browsing history, geolocation data, fingerprints, and inferences from other personal information that could create a profile about your preferences and characteristics.").

72. While beyond the scope of this Note, it bears mentioning that Europe's General Data Protection Regulation suffers from similar limitations as U.S. biometric laws, as its definition for biometrics also privileges identification through facial and fingerprint scans. *See* Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 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), art. 4, 2016 O.J. (L 119) 3.

73. 740 ILL. COMP. STAT. 14/1 (2008).

74. TEX. BUS. & COM. § 503.001 (West 2017).

75. WASH. REV. CODE § 19.375 (2017).

76. CAL. CIV. CODE § 1798.150(a)(1) (2021).

77. Ienca et al., *supra* note 49, at 2.

78. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 598–99 (2011).

Commission's over-emphasis on transparency privileges companies' unilateral option to prescribe their data practices, with little recourse for consumers to meaningfully opt out without losing access to the companies' services.[79] Absent substantive protections, privacy law remains a self-governing regime that allays meaningful choice and enforces a regulative ideal that we can and do read consumer-facing privacy policies, evaluate the choices available to us, and make informed choices. Yet it seems like an overestimation to assume that reading and understanding how platforms collect our data will inure to any substantive policy overhauls.[80]

Given the current privacy landscape, the FTC—and even state attorneys general (AGs)—can only offer limited protections for consumer data privacy.[81] Their efforts largely operate within existing legal infrastructures captured by corporate interests in self-regulation. As Woodrow Hartzog noted, building privacy frameworks around concepts of transparency and informational self-determination impresses the idea that consumers exercise autonomy in their online interactions.[82] However, when platforms obscure or subvert the availability of choices,[83] neither state AGs nor the FTC can signal particular harms. Our existing notice-and-consent regime thereby turns informed consent into a platitude, allocating risk management to consumers whose choices are ill-defined and illusive.[84]

Inadequate legal infrastructures are part and parcel of the broader political economy that enables corporate actors to operate within the confines of the law.[85] As Ari Waldman argued, privacy law reaches its apex when judges, lawyers, and scholars defer to symbolic structures—appointing compliance

---

79. *Id.* at 599.

80. *See* Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1500 (2019).

81. *See* Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 784 (2020); *see also* Richards & Hartzog, *supra* note 80, at 1499.

82. Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, *in* REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS 96, 102 (Amba Kak ed., 2020).

83. For discussions of user interface designs that deceive users into making unintended, harmful choices, see generally Arunesh Mathur, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty & Arvind Narayanan, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 PROC. ACM HUM.-COMPUT. INTERACTION 1 (2019) (uncovering entities that offer dark patterns as a turnkey solution); Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'*, 31 CURRENT OPINIONS PSYCH. 105 (2020) (highlighting cognitive biases and discussing the ways in which platform design can manipulate disclosure behavior).

84. *See* Hartzog, *supra* note 82, at 103.

85. *See* Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460, 1465 (2020).

officers, conducting data risk assessments and impact evaluations, and automating data breach notifications—as evidence of adherence to the law.[86] All the law does, then, is transfer regulatory monitoring to companies themselves, wedding a form of collaborative governance that shifts compliance enforcement out of regulators' hands.[87] Meanwhile, standard-setting organizations for emerging technologies—such as the Institute of Electrical and Electronics Engineers and the Organization for Economic Co-operation and Development—construct rules that blindly favor innovation and dispense with substantive consumer protections. These organizations thereby tout the same platitudes around ethics and transparency, entrenching companies' discursive apparatus.[88] Under this rubric, companies perform compliance for its own sake, circumventing legal scrutiny and disabling regulators from targeting—let alone identifying—companies' more deleterious practices.[89]

V. TOWARDS AN EMANCIPATORY FRAMEWORK FOR REGULATING BCIS

Well-meaning critics in technology policy circles espouse the view that the law lags behind emerging technologies.[90] But this view undermines how companies rely upon law to exercise power and shift the normative discourses that further entrench it.[91] It also fails to appreciate what law can protect. Legal regimes are better equipped to protect external manifestations, such as verbal utterances and written texts.[92] They are less able to govern internal practices, such as unspoken information, preconscious preferences, attitudes, and beliefs.[93] For this reason, neural data throws traditional precepts for privacy law into a frenzy. Unlike most protected categories of information, it pertains to unexecuted behavior, inner speech, or non-externalized actions that elude conscious control and prove difficult to intentionally seclude.[94] Indeed, the

86. *See* Waldman, *supra* note 81, at 815.

87. *Id.*; *cf.* Waldman, *supra* note 11, at 1227 ("Perhaps most importantly, the performative use of a managerialized public-private partnership is internally inconsistent: it endogenously creates public institutions that are dependent on industry expertise, efficiency, and nimbleness. Therefore, those public institutions become incapable of acting as the promised 'backdrop threat' that guards against capture.").

88. *Cf.* Waldman*, supra* note 9, at 1242–43 (discussing privacy's collaborative governance model between public and private actors).

89. Waldman, *supra* note 81, at 815.

90. ZUBOFF, *supra* note 63, at 103.

91. *See* Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460, 1465 (2020); *see also* COHEN, *supra* note 68, at 44.

92. Ienca et al., *supra* note 49, at 6.

93. *Id.* at 6–7.

94. *Id.* at 6.

process of extracting neural data compels disclosures that users retain interest in self-regulating. Resistance against these emerging forms of corporate manipulation therefore requires multivalent approaches.

First, attempts to remedy BCIs' privacy harms must draw attention to the technology's data practices. Recently, privacy professionals have endeavored to operationalize data minimization principles to reduce the extent of data required to empower their technologies and delete such data once they completed using it for its intended purposes. But the principle remains a platitude so long as it remains abstract and without context. Indeed, while it may guide privacy professionals to think more intentionally about their data practices, it does little to inform or constrain data practices themselves, including collection, disclosure, and retention. To paraphrase Ari Waldman, privacy professionals converted data minimization into a performative gesture to reduce regulatory investigations and litigation; that is, the principle became understood more in terms of reducing "corporate risk" than risks to consumers.[95]

Second, advances in legal protections only remain viable to the extent that they parallel ongoing engagement with neuro-ethicists, human rights advocates, and other stakeholders. For example, the Morningside Group comprises a team of interdisciplinary experts—including physicians, ethicists, neuroscientists, and computer scientists—that structured a set of human rights-centered ethical principles to guide research on BCIs and provide technical know-how to lawmakers.[96] Applying a multi-stakeholder perspective, these varying areas of expertise converge to produce more robust understandings of near- and long-term implications for emerging neurotechnologies. As such, regulators should rely on researchers in the BCI space to play an integral and ongoing role in informing legal frameworks for protecting neural data, ensuring that these frameworks keep pace with the technology's innovation.

Finally**,** on the legal side, protections for our neural data must strive to articulate safeguards to mental privacy, personal identity, free will, and

95. *See* Waldman, *supra* note 81, at 800.

96. Rafael Yuste, Sara Goering, Blaise Agüera y Arcas, Guoqiang Bi, Jose M. Carmena, Adrian Carter, Joseph J. Fins, Phoebe Friesen, Jack Gallant, Jane E. Huggins, Judy Illes, Philipp Kellmeyer, Eran Klein, Adam Marblestone, Christine Mitchell, Erik Parens, Michelle Pham, Alan Rubel, Norihiro Sadato, Laura Specker Sullivan, Mina Teicher, David Wasserman, Anna Wexler, Meredith Whittaker & Jonathan Wolpaw, *Four Ethical Priorities for Neurotechnologies and AI*, 551 NATURE 159, 160 (2017).

equitable access to technologies that augment human capacities.[97] As of October 2021, Chile became the first country to protect these "neuro-rights," pioneering a regulatory framework to govern against manipulation of brain activity.[98] Chile amended its constitution to define mental identity as a right against manipulation. The right requires that any intervention—including for medical purposes—must be regulated.[99]

As the first country to protect neuro-rights, Chile sets an example for others to emulate. In addition to its constitutional amendment, the country modeled several principles that apply across all contexts for BCI development. First, Chile's right to mental privacy develops a starting point for ensuring the secure collection and maintenance of neural data. Any sale, commercial transfer, or use of neural data must adhere to strict regulation. Second, users retain a right in personal identity, such that technologies may not interfere with users' sense of self. This may occur when, for example, users are incapable of processing whether their actions derive from personal or technological input. Third, providing for a right to free will, Chile requires that users retain control over their own decision-making capacity without unknown influence from external devices. And finally, by granting a right to equal access to mental augmentation, the country seeks to establish guidelines at domestic and international levels for regulating the development and application of BCI devices.

To the extent that existing privacy laws prove insufficient in their definitions and scope to protect neural data, regulators should consider explicit protections for such data in advance of BCIs' fast-paced development. Such prophylactic regulation informs technological development and ensures that it maintains an emphasis on users' safety and privacy interests. In this instance, innovation may not be at odds with regulation; the two would co-develop BCI technologies so that they enable users to experience a diversity of human experiences.

As technological development draws human-machine synergies nearer, regulators have ample opportunity to ensure that such technologies enhance rather than displace these experiences. These efforts should, on the one hand,

97. Neeraja Seshadri, *Chile Becomes First Country to Pass Neuro-Rights Law*, JURIST (Oct. 2, 2021), https://www.jurist.org/news/2021/10/chile-becomes-first-country-to-pass-neuro-rights-law/.

98. Nayef Al-Rodhan, *The Rise of Neurotechnology Calls for a Parallel Focus on Neurorights*, SCI. AM. (May 27, 2021), https://www.scientificamerican.com/article/the-rise-of-neurotechnology-calls-for-a-parallel-focus-on-neurorights/.

99. Elena Blanco-Suarez, *"Neurorights" and Why We Need Them*, PSYCH. TODAY (June 25, 2020), https://www.psychologytoday.com/us/blog/brain-chemistry/202006/neurorights-and-why-we-need-them.

enable the expansion of medical and rehabilitative uses while, on the other hand, limiting the use and disclosure of neural data to only the data controllers and their vendors that are necessary to ensure the devices' functionality. In short, this limits the possible disclosures for neural data and offsets the possibility that such data will be used for ancillary third-party purposes, such as profiling, targeted advertising, or behavioral analytics.

Finally, regulators should broaden enforcement efforts with a private right of action. Elsewhere I have argued that a private right of action empowers consumers to protect their privacy without regulators' intervention.[100] Rather than rely on under-resourced enforcement agencies, consumers should leverage such a private right of action as a self-help mechanism for shaping industry behaviors. Indeed, while regulators may set the foundation in law for consumer protections, consumers—with the aid of the plaintiffs' bar—may take the mantle in courts to ensure adequate enforcement for mental privacy.

VI. CONCLUSION

At their core, BCIs dispossess users of their thoughts and displace them from the mind into actionable outputs. Through this digital process, the space between intention and action draws nearer, eliminating the antecedent reflective capacity necessary to instantiate action. As this Note discussed, the result fundamentally reconstitutes our person into an assemblage of disembodied agency, wherein the body acts through a sequence of automatisms. Such automatisms habituate thought and delimit the possibility to engage in conscious reflection, the precursor to meaningful expression.

As Anders Dunker wrote, "the brain has become the nexus of an intensified political struggle due to the repercussions of cognitive capitalism."[101] Our political economy enables companies to engage in uninhibited data extraction, with deficits in legal infrastructure privileging such practices. Where the law lacks, government actors defer to industry self-regulation that, in turn, informs the normative underpinnings to doing privacy. Indeed, in the absence of substantive policy overhauls—at the legal and normative levels—companies' power to manipulate our social embodiments will continue unchecked.

Perhaps most critically, resistance must engage with existing liberatory practices on the ground. The problem exceeds the emergence of any particular

100. *See* Daniel Levin, *Face the Fact, or Is the Face a Fact?: Biometric Privacy in Publicly Available Information*, 32 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1010, 1015 (2022).

101. Anders Dunker, *The Neural Battlefield of Cognitive Capitalism*, L.A. REV. BOOKS (Nov. 6, 2020), https://lareviewofbooks.org/article/the-neural-battlefield-of-cognitive-capitalism/.

technology; it traces a longstanding political struggle against total administration. Indeed, as the Marxist adage goes: to be radical is to grasp the root of the matter.[102] Writing in 1964, Herbert Marcuse articulated how a burgeoning technological society generated false needs and integrated consumers into its world of thought and behavior.[103] Through existing systems of production and consumption, emerging innovations engender corporate power and displace aptitudes for critical thought, producing "mechanics of conformity" that assimilate consumers into a one-dimensional universe predicated on corporate norms.[104] For Marcuse, the only adequate solution requires the "Great Refusal—the protest against that which is."[105]

Today, practicing the Great Refusal requires us to deconstruct what Alex Campolo and Kate Crawford called "enchanted determinism"—the epistemological flattening of complexity into clean signal for the purposes of prediction.[106] As Crawford wrote, emerging technologies—especially those integrating AI and machine learning—are seen as enchanted yet deterministic, deducing patterns that we treat with predictive certainty.[107] Shrouded in veneers of science and truth, these technologies sublimate existing power structures and invert the starting assumption that these technologies act on us, taxing our limited attentional flows.

Under this rubric, emerging uses for neurotechnologies perpetuate age-old privacy concerns, undermining our integrity to exercise agency in and through our person. Positioning their growing innovation in this context enables us to identify how companies recapitulate profit motivations through new forms of data extraction and manipulation. By ascribing an essential interiority to our person, these technologies not only predict, but preempt the possibilities to exercise alternative subjectivities. Legislating new protections for new categories of data offer a starting point, however insufficient they may be. But the struggle calls for a grander vision, one that imagines new ways of relating to each other absent corporate-facilitated mediations and technologies.

---

102. KARL MARX, EARLY WRITINGS 52 (Rodney Livingstone & Gregor Benton trans., 1992).

103. HERBERT MARCUSE, ONE-DIMENSIONAL MAN xii (Beacon Press 1991).

104. *Id.* at xx.

105. *Id.* at 66.

106. CRAWFORD, *supra* note 48, at 213.

107. *Id.*