UNIVERSITY *of* PENNSYLVANIA
JOURNAL *of* LAW & PUBLIC AFFAIRS

Vol. 7 May 2022 No. 2

MIND GAMES: HOW ROBOTS CAN HELP REGULATE BRAIN-COMPUTER INTERFACES

Elle Rothermich *

---

* Editor-in-Chief, *University of Pennsylvania Journal of Law & Public Affairs*; University of Pennsylvania Law School, J.D. Candidate, 2022; Perelman School of Medicine, M.B.E. Candidate, 2022; Cornell University, B.A., 2019. My deepest gratitude to Professor Anna Wexler for her thoughtful mentorship and to Professor Paul Heaton, Jeanne Rothermich, and Sumita Rajpurohit for their extremely helpful review. Many thanks to the staff of the *University of Pennsylvania Journal of Law & Public Affairs* for their careful editing. All errors and omissions are my own.

INTRODUCTION

In April 2021, Neuralink, Elon Musk's neurotechnology company, released a YouTube video purporting to show a monkey playing the video game Pong using his thoughts instead of a handheld controller.[1] According to voiceover narration in the video, the monkey was able to do this thanks to an implanted device called a "Neuralink" that allows the brain to communicate directly with technology outside the brain.[2] The company has tested a version of the device in pigs but not in humans.[3]

Musk has been vocal about his hopes for Neuralink technology. In a series of tweets, he predicted that the first Neuralink products "will enable someone with paralysis to use a smartphone with their mind faster than someone using thumbs" while "[l]ater versions will be able to shunt signals from Neuralinks in brain to Neuralinks in body motor/sensory neuron clusters, thus enabling, for example, paraplegics to walk again."[4] For those worried about what a Neuralink might feel like, he added that the "device is implanted flush with the skull" so users will "feel totally normal."[5]

Most research into brain-computer communication focuses on giving people with limited motor function more control over their environment. But Musk thinks that Neuralink has potential as a consumer product, too.[6] Facebook, not to be left out of the fun, announced development of a commercially available thought-to-text device around the same time Musk announced Neuralink. Facebook has since abandoned plans for such a device in favor of a virtual reality controller that uses similar technology but "has a nearer-term path to market."[7]

---

[1] Elizabeth Lopatto, *Watch: Elon Musk's Neuralink Says This Monkey is Playing Pong with Its Mind*, THE VERGE (Apr. 8, 2021), https://www.theverge.com/2021/4/8/22374749/elon-musk-neuralink-monkey-pong-brain-interface [https://perma.cc/F5RP-HBZS].

[2] *Id.*

[3] Tanya Lewis, *Elon Musk's Pig-Brain Implant Is Still a Long Way from 'Solving Paralysis'*, SCI. AM. (Sept. 2, 2020), https://www.scientificamerican.com/article/elon-musks-pig-brain-implant-is-still-a-long-way-from-solving-paralysis/ [https://perma.cc/H926-76BD].

[4] Elon Musk (@elonmusk), TWITTER (Apr. 8, 2021, 8:24 PM), https://twitter.com/elonmusk/status/1380315654524301315?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1380315654524301315%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.theverge.com%2F2021%2F4%2F8%2F22374749%2Felon-musk-neuralink-monkey-pong-brain-interface [https://perma.cc/9VFT-62NL].

[5] *Id.*

[6] *Id.*; *see also Applications*, NEURALINK, https://neuralink.com/applications/ [https://perma.cc/NY9J-4ZGH] (last visited Jan. 7, 2022) ("This technology has the potential . . . eventually to expand how we interact with each other, with the world, and with ourselves.").

[7] Antonio Regalado, *Facebook is Ditching Plans to Make an Interface that Reads the Brain*, MIT TECH. REV. (July 14, 2021), https://www.technologyreview.com/2021/07/14/1028447/

An increasing number of neurotechnology-focused companies have appeared over the past decade or so.[8] In case you would prefer not to wear a health tracker on your wrist, many of these companies offer FitBit-like products that you wear on your head.[9] Some of this consumer neurotechnology stimulates the brain with electrical signals.[10] Other products allow the user to interact with the outside world, to a limited degree, using their thoughts alone.[11] Most, however, are best understood as health trackers—they record a sampling of your brain waves and send that sampling to an app which tells you (in theory) how you are feeling or offers some other insight into your health.[12]

These consumer products cannot "read minds" in the way most of us understand the phrase. They cannot delve into your psyche to provide a nuanced report of your emotions.[13] They need a lot of assistance to play the "guess the number I'm thinking" game.[14] Unlike their lab-based cousins, they

---

facebook-brain-reading-interface-stops-funding/ [https://perma.cc/XZQ2-232H]. Facebook's funding did find some success, however. In 2021, a Facebook-funded team announced it had "decode[d] words and sentences directly from the cerebral cortical activity" of someone unable to speak (i.e., anarthria) with a neuroprosthesis and deep-learning algorithms. David A. Moses, Sean L. Metzger, Jessie R. Liu, Gopala K. Anumanchipalli, Joseph G. Makin, Pengfei F. Sun, Josh Chartier, Maximilian E. Dougherty, Patricia M. Liu, Gary M. Abrams, Adelyn Tu-Chan, Karunesh Ganguly & Edward F. Chang, *Neuroprosthesis for Decoding Speech in a Paralyzed Person with Anarthria*, 385 NEW ENG. J. MED. 217, 217 (2021).

[8] Cathy Hackl, *Meet Ten Companies Working on Reading Your Thoughts (and Even Those of Your Pets)*, FORBES (June 21, 2020), https://www.forbes.com/sites/cathyhackl/2020/06/21/meet-10-companies-working-on-reading-your-thoughts-and-even-those-of-your-pets/?sh=44508082427c [https://perma.cc/33RX-B3LZ].

[9] *Id.*

[10] Anna Wexler & Peter B. Reiner, *Oversight of Direct-to-Consumer Neurotechnologies*, 363 SCIENCE 234 (2019).

[11] *The Force Trainer II: Hologram Experience*, NEUROSKY, https://store.neurosky.com/#other-products [https://perma.cc/L6DK-GCRP] (last visited Jan. 7, 2021) ("Use the power of your mind to move holograms and perform amazing feats of Jedi strength from different Star Wars movies. Real brainwave sensors on the wireless headset detect the strength of your concentration from your brainwaves and trigger changes in the hologram.").

[12] *E.g.*, *Choose Muse*, MUSE, https://choosemuse.com/ [https://perma.cc/767L-XA2M] (last visited Jan. 7, 2021) [hereinafter MUSE].

[13] Anna Wexler & Robert Thibault, *Mind-Reading or Misleading? Assessing Direct-to-Consumer Electroencephalography (EEG) Devices Marketed for Wellness and Their Ethical and Regulatory Implications*, 3 J. COGNITIVE ENHANCEMENT 131, 134–35 (2019).

[14] *See* Jordan J. Bird, Diego R. Faria, Luis J. Manso, Anikó Ekárt & Christopher D. Buckingham, *A Deep Evolutionary Approach to Bioinspired Classifier Optimisation for Brain-Machine Interaction*, 2019 COMPLEXITY 4316548 (2019), at 12, https://www.hindawi.com/journals/complexity/2019/4316548/ [https://perma.cc/VC5X-EU3Z] (reporting that a novel computational model, using a brain signal dataset developed with the Muse headband, could generate accurate guesses in a number-guessing experiment less than forty percent of the time).

cannot produce fuzzy reconstructions of what a user sees by measuring signals from a part of the brain's visual cortex.[15]

Nevertheless, these consumer neurotechnology products may be dangerous.[16] As FDA's mandate covers "medical devices" but not "wellness devices," many of these products go unregulated.[17] Not every "neurotechnology" product is deserving of the label. Neurotechnology companies often over-sell their products, promising everything from better sleep to higher intelligence.[18] These are current, pressing issues. The market for these products is growing—fast. Regulation and more attention from policymakers are sorely needed.[19]

But ensuring that regulation is effective will be a tall order. Devices that enable direct communication between the brain and computers are a large, complex, and quickly developing class of neurotechnologies. Although few are capable of anything near "mind reading," media coverage of Neuralink and research breakthroughs has inspired widespread anxiety that private thoughts will soon be publicly accessible. This mix of complex technology, real-life advances, and sci-fi expectations makes it hard to pin down what these devices are—and what they are really capable of. How do you regulate technologies that seem to elude definition?

Bryan Casey and Mark A. Lemley have an idea. In *You Might Be A Robot*, they argue that when it comes to regulating robots or artificial intelligence, trying to pinpoint an objective definition leads to under-regulation, over-regulation, and rapid obsolescence.[20] They suggest regulating conduct instead of trying to find the perfect definition of "robot"—in other words, regulating "verbs, not nouns" by developing functional criteria in place of exact definitions.[21] When it is really necessary to decide whether something is a robot, they propose making case-by-case

---

[15] Shinji Nishimoto, An T. Vu, Thomas Naselaris, Yuval Benjamini, Bin Yu & Jack L. Gallant, *Reconstructing Visual Experiences from Brain Activity Evoked by Natural Movies*, 21 CURRENT BIOLOGY 1641, 1646 (2011). *See also* Moises Velasquez-Manoff, *The Brain Implants that Could Change Humanity*, N.Y. TIMES (Aug. 28, 2020), https://www.nytimes.com/2020/08/28/opinion/sunday/brain-machine-artificial-intelligence.html [https://perma.cc/N82Z-U9FG] (describing experiment and limitations of currently available consumer technologies).

[16] *See* Marcello Ienca, Pim Haselager & Ezekiel J Emanuel, *Brain Leaks and Consumer Neurotechnology*, 36 BIOTECHNOLOGY & NATURE 805, 805 (2018) (arguing that "[g]reater safeguards are needed to address the personal safety, security and privacy risks arising from increasing adoption of neurotechnology in the consumer realm").

[17] FOOD & DRUG ADMIN., GENERAL WELLNESS: POLICY FOR LOW RISK DEVICES 2 (2019) [hereinafter POLICY FOR LOW RISK DEVICES].

[18] Anna Wexler & Robert Thibault, *supra* note 13, at 133.

[19] *Id.* at 136; Marcello Ienca, Pim Haselager & Ezekiel J Emanuel, *supra* note 16, at 808–10.

[20] Bryan Casey & Mark A. Lemley, *You Might Be a Robot*, 105 CORNELL L. REV. 287 (2020) [hereinafter *You Might Be a Robot*].

[21] *You Might Be a Robot*, *supra* note 20, at 342.

determinations and striving to keep definitions "as short term and contingent as possible."[22] Regulators and courts, they argue, are better equipped to make such determinations than legislatures.[23] If specific legislation is ever needed, legislators should add safeguards that allow them to adjust provisions to keep up with ever-evolving technology.[24]

"Brain-computer communication device" may be a little easier to define than "robot," if only because it encompasses a smaller group of things.[25] However, depending on one's point of view, "brain-computer communication device" may be overbroad or too narrow. This comment uses the term "brain-computer interface" (BCI) because it is common in both expert and non-expert writings about this technology. (You probably gathered that from the title.) The broad use of BCI here is meant to ease reading, not as an argument about what the scope of the term should be in papers dealing with the technical aspects of connecting brains with computers. This is not one of those papers.

This comment explores the application of Casey and Lemley's thesis to the definitional problem that devices described above present. Part I surveys recent developments in BCI technology, the limits of currently available consumer BCIs, and the challenges of regulating emergent technologies. It concludes with an overview of growing concerns about the privacy risks of BCIs—a "privacy narrative"—that whether true, exaggerated, or somewhere in between is a big reason why defining "BCI" for regulatory purposes is difficult. Part II delves into *You Might Be A Robot* and makes the case for treating BCIs the way Casey and Lemley propose robots should be treated. It also adds "affect" to Casey and Lemley's list of suggested functional criteria for robot regulation. Affect is a consideration of the way that people are likely to react to a given technology, such as a robot police dog or a BCI device. Because affect can differ significantly from "agenda"—that is, what a technology is actually meant to do—it may be a useful tool for effectively regulating new technologies like BCIs.

I. NEURONS AND NARRATIVES

This section will first provide a brief scenic tour of the basics of BCI technology, recent developments, and the limits of currently available consumer BCI products. I will then present a brief explanation for why regulating BCIs and similar technologies can be difficult. My goal here is twofold. First, I hope to demystify BCIs, if only slightly. Second, I aim to lay

---

[22] *Id.* at 295.
[23] *Id.*
[24] *Id.*
[25] *See infra* Part II.

a foundation for Part II by introducing the gap between what BCIs can do and what people think they can do. This gap, I argue in Part II, likely will require regulators and industry actors to take affect—how people respond emotionally to something—into account when (self-)regulating.

A. Brain-Computer Interfaces

1. What are they?

Neuralink is not the first company to develop devices that connect brains and computers. The basic technology is older than you might think. Back in 1973, UCLA professor Jacques Vidal published "Toward Direct Brain-Computer Communication" in the *Annual Review of Biophysics and Bioengineering*.[26] Since then, research teams have developed a number of "thought-to-application" devices, including "thought-controlled" robotic arms and drones.[27] A few have investigated ways of "writing" the brain, such as controlling epileptic seizures.[28] In mid-2020, a team associated with the long-running BrainGate project announced that they had created a device that could translate the user's imagined handwriting movements into text in real time.[29] In early 2021, the U.S. Food and Drug Administration (FDA) authorized marketing the "Neurolutions IpsiHand Upper Extremity Rehabilitation System" for people with reduced hand, wrist, or arm

---

[26] Jacques J. Vidal, *Toward Direct Brain-Computer Communication*, 2 ANN. REV. BIOPHYSICS & BIOENGINEERING 157 (1973).

[27] *E.g.*, *BrainGate Publication Timelines*, BRAINGATE (Jan. 7, 2021), https://www.braingate.org/publications-timeline/ [https://perma.cc/3S25-SARE]; Emily Durham, *First-Ever Noninvasive Mind-Controlled Robotic Arm*, CARNEGIE MELLON C. ENGINEERING (June 20, 2019), https://engineering.cmu.edu/news-events/news/2019/06/20-he-sci-robotics.html [https://perma.cc/5P45-8YMY].

[28] Liam Drew, *Agency and the Algorithm*, 571 NATURE S19 (2019).

[29] Francis R. Willett, Donald T. Avansino, Leigh R. Hochberg, Jaimie M. Henderson & Krishna V. Shenoy:

> Here, we demonstrate an intracortical BCI that can decode imagined handwriting movements from neural activity in motor cortex and translate it to text in real-time, using a novel recurrent neural network decoding approach. With this BCI, our study participant (whose hand was paralyzed) achieved typing speeds that exceed those of any other BCI yet reported: 90 characters per minute at >99% accuracy with a general-purpose autocorrect. These speeds are comparable to able-bodied smartphone typing speeds in our participant's age group (115 characters per minute) and significantly close the gap between BCI-enabled typing and able-bodied typing rates.

High-Performance Brain-to-Text Communication via Handwriting, 593 NATURE 249, 249 (2021).

movement caused by a stroke.[30] This prescription-only system records a user's brain activity, analyzes it to determine what muscle movement the user intended, and then signals a hand brace to move the user's hand accordingly.[31]

It should be noted that experts tend to use the term BCI to describe a smaller group of devices than non-experts do. At a high level of generality, a BCI is a device that allows a brain and a computer to directly interface, or connect, with each other. BCIs overlap in form and function with other kinds of neurotechnology, such as neurostimulation[32], neuroimaging[33], and multi-purpose wearable health trackers.[34] Neuroimaging does not involve connecting brains and computers unless you really stretch the meaning of "connect." However, the line between devices that virtually everyone agrees are BCIs and other neurotechnologies can be fuzzy. Many experts, but not all, distinguish neurostimulation and BCIs.[35] Wearable health trackers that use EEG (electroencephalography) are usually classified as BCIs, but trackers that indirectly measure brain activity, such as through blood oxygen measurements, may not be. In a 2014 workshop, FDA defined BCIs as "neuroprostheses that interface with the central or peripheral nervous system to restore lost motor or sensory capabilities."[36] This definition covers IpsiHand, but it obviously does not cover devices that are meant to give their users capabilities beyond those that are biologically possible, such as the Muse headband or Neuralink.

This is not to say that FDA's definition is wrong, or that any definition is wrong. Rather, I mention this fuzziness to lay the foundation for the second Part of this comment. In "You Might Be A Robot," Casey and Lemley present a comprehensive overview of the challenges facing policymakers, regulators, and pretty much everyone else who tries to come up with a perfect definition of "robot."[37] I do not have room for a similarly comprehensive overview of the challenges of defining "BCI." Accordingly, this Comment uses "a device

---

[30] Press Release, Food & Drug Admin., FDA Authorizes Marketing of Device to Facilitate Muscle Rehabilitation in Stroke Patients (Apr. 23, 2021), https://www.fda.gov/news-events/press-announcements/fda-authorizes-marketing-device-facilitate-muscle-rehabilitation-stroke-patients [https://perma.cc/5RGW-5R6B].
[31] *Id.*
[32] Anna Wexler & Robert Thibault, *supra* note 13; Ienca et al., *supra* note 16.
[33] Ienca et al., *supra* note 16.
[34] Karola V. Kreitmair, *Dimensions of Ethical Direct-to-Consumer Neurotechnologies*, 10 AJOB NEUROSCIENCE 152, 154 (2019).
[35] Anna Wexler & Robert Thibault, *supra* note 13; Ienca et al., *supra* note 16. *But see* Kreitmair, *supra* note 34 (including VR devices in survey of neurotechnologies).
[36] FOOD & DRUG ADMINISTRATION, DISCUSSION PAPER: BRAIN-COMPUTER INTERFACE (BCI) DEVICES FOR PATIENTS WITH PARALYSIS AND AMPUTATION 3 (2014), https://www.fda.gov/media/116776/download#page=3 [https://perma.cc/5L6W-K9ZD].
[37] Bryan Casey & Mark A. Lemley, *supra* note 20, at 342.

that allows a brain and a computer to interface directly" as a working definition.

2. How do they work?

Most BCIs share a few basic components: hardware that physically interfaces with the brain (including the electrode array); an electrical amp; analytic software to detect brain activity; and communication and feedback monitoring systems.[38] BCIs with these components usually rely on EEG or another method of detecting electrical brain activity.[39] Some BCIs, however, use nonelectric detection methods such as fNIRs and fMRIs.[40] These measure "task-induced blood oxygen-level dependent responses," which correlate with brain activity.[41]

BCIs of all types often employ machine learning algorithms—artificial intelligence (AI)—to classify brain signals and turn those signals into an output, such as moving a cursor on a computer screen.[42] AI can also serve an "auto-complete" or "auto-correct" function to increase a BCI's accuracy.[43]

BCIs that use electrodes can detect various kinds of electrical brain activity, with various levels of accuracy, depending on where the electrodes are placed.[44] As you might expect, invasive (internal) BCIs receive better

---

[38] OWEN D. JONES, JEFFERY D. SCHALL & FRANCIS X. SHEN, LAW AND NEUROSCIENCE 825–28 (2d ed. 2021); *see* Andreas Wolkenstein, Ralf J. Jox & Orsolya Friedrich, *Brain-Computer Interfaces: Lessons to be Learned from the Ethics of Algorithms*, 27 CAMBRIDGE Q. HEALTHCARE ETHICS 636, 636 (2018) (describing BCIs as consisting of four elements: (1) the user's generation of brain signals; (2) "the measurement of these signals"; (3) "the decoding of the measured brain signals"; and (4) "the output commands that direct a given external device").

[39] JONES et al., *supra* note 38.

[40] Ranganatha Sitaram, Sangkyun Lee & Niels Birbaumer, *BCIs That Use Brain Metabolic Signals*, *in* BRAIN-COMPUTER INTERFACES: PRINCIPLES AND PRACTICE 301 (Jonathan Wolpaw & Elizabeth Winter Wolpaw eds., 2012).

[41] *Id.*

[42] *See* Wolkenstein, Jox & Friedrich, *supra* note 38, at 636–37 (listing the steps of BCI functioning in which algorithms may be found).

[43] *Id.* at 637. See *infra* Part II (for a more in-depth discussion of the benefits and risks of this particular use of AI).

[44] JONES et al., *supra* note 38, at 826. See Wolkenstein, Jox & Friedrich, *supra* note 38, at 636, noting the common division of BCIs into three categories:

> [A]ctive BCIs in which the user intentionally produces certain brain states (e.g., motor imagery) that the BCIs learn to connect with the intended output; reactive BCIs in which the user is presented with certain (mostly visual or auditive) stimuli while the BCI measures a particular reactive brain signal; and passive BCIs in which the user's brain activity is monitored and action is taken as soon as a predefined state occurs.

signals from the brain than noninvasive (external) BCIs.[45] Invasive BCIs employ electrode arrays that sit in the brain. They can "read" the activity of a small group of neurons or even a single neuron.[46] This requires delicate, invasive surgery to place the electrodes near the target neurons.[47] In contrast, noninvasive BCIs employ EEG sensors that do not penetrate the skull. These BCIs "read" the activity of a large group of neurons.[48] There are also BCIs that employ ECoGs, which sit on top of the brain under the skull, as compromise between internal and external BCIs.[49]

It is easier to get detailed signals when a skull is not in between the sensor and the targeted neurons. More detailed signals produce better outputs. This means that, in general, invasive BCIs are capable of more complex tasks than noninvasive BCIs. For example, someone using an external BCI may be able to slowly move a robot arm in four directions after intensive training. Using an internal BCI, that same person may be able to move a robot arm, after less training, in more than four directions with similar speed and fluidity as a person with no motor challenges can move their own arm.[50]

Researchers are still working to determine whether signal detail alone limits the BCI user's control of the device.[51] In addition, both academic and commercial labs have increasingly turned to machine learning—a type of AI—to create BCIs capable of carrying out more complex tasks.[52] Machine learning allows noninvasive BCIs to take in less precise signals and guess what detail is missing. This ability to interpret brain signals is a big reason why BCIs are a high-potential, high-risk technology. While machine learning has yet to allow noninvasive BCIs to surpass invasive BCIs when it comes to complex tasks, it will likely have a major impact on the type of noninvasive BCIs available to consumers in the near future.

Certain brain activity signals are particularly suited for BCIs: P300 event-related potentials; sensorimotor rhythms; steady-state visual evoked

---

[45] JONES et al., *supra* note 38.
[46] John P. Donoghue, *BCIs That Use Signals Recorded in Motor Cortex*, *in* BRAIN-COMPUTER INTERFACES: PRINCIPLES AND PRACTICE 278 (Jonathan Wolpaw & Elizabeth Winter Wolpaw eds., 2012); Hansjörg Scherberger, *BCIs That Use Signals Recorded in Parietal or Premotor Cortex*, *in* BRAIN-COMPUTER INTERFACES: PRINCIPLES AND PRACTICE 293 (Jonathan Wolpaw & Elizabeth Winter Wolpaw eds., 2012).
[47] Donoghue, *supra* note 46.
[48] Gerwin Schalk, *BCIs That Use Electrocorticographic Activity*, *in* BRAIN-COMPUTER INTERFACES: PRINCIPLES AND PRACTICE 251 (Jonathan Wolpaw & Elizabeth Winter Wolpaw eds., 2012).
[49] *Id.*
[50] Schalk, *supra* note 48, at 257.
[51] *Id.* at 257–59.
[52] *See, e.g.*, Durham, *supra* note 27; Schalk, *supra* note 48, at 257.

potentials; and error-related negative evoked potentials.[53] Although the particulars of these signals are of limited importance to this Comment's main purpose, I offer a brief overview of each to illuminate which BCIs are likely to enter the consumer market in the near future, which are not, and what functionality BCIs actually offer. As researchers continue to uncover more about the brain and what it can tell us about the mind, other brain signal types may come to the fore.

P300 event-related potentials appear at the scalp 250 to 700 milliseconds after someone detects that a rare or desired event has occurred.[54] Finding and clicking on the internet browser on your computer generates a P300 potential, as does hearing a song you recognize. P300-based BCIs are portable, have inexpensive hardware, require minimal training, and take only minutes to set up for a new user.[55] Although P300-based BCIs are rare on the consumer market, they could be employed as direct-to-consumer thought-to-text devices.

Over the course of decades, neuroscientists discovered and then confirmed an association between voluntary movements and specific wave frequencies now known as sensorimotor rhythms (SMRs).[56] More research uncovered a correlation between SMRs and *imagining* movement, clearing the way for the development of SMR-based BCIs.[57] Unlike P300-based BCIs, which track an involuntary response, SMR-based BCIs require users to think about something specific.[58] This can require substantial training for both the user and the BCI.[59] Developers must also ensure that the BCI is programmed to distinguish the targeted SMRs from electrical activity produced by muscles in the scalp, face, and neck.[60] Despite these drawbacks, SMR-based BCIs could work well for people who are missing limbs or have limited mobility.[61]

---

[53] Anastasia Greenberg, *Inside the Mind's Eye: An International Perspective on Data Privacy Law in the Age of Brain-Machine Interfaces*, 29 ALB. L.J. SCI. & TECH. 79, 84 (2019).
[54] Eric W. Sellers, Yael Arbel, Emanuel Donchin, *BCIs That Use P300 Event-Related Potentials*, *in* BRAIN-COMPUTER INTERFACES: PRINCIPLES AND PRACTICE 216 (ed. Jonathan Wolpaw & Elizabeth Winter Wolpaw) (2012).
[55] *Id.* at 215.
[56] Gert Pfurtscheller & Dennis J. McFarland, *BCIs That Use Sensorimotor Rhythms*, *in* BRAIN-COMPUTER INTERFACES: PRINCIPLES AND PRACTICE 227 (Jonathan Wolpaw & Elizabeth Winter Wolpaw eds., 2012).
[57] *Id.* at 228.
[58] *Id.*; Wexler & Thibault, *supra* note 13, at 134–35.
[59] Pfurtscheller & McFarland, *supra* note 56, at 233.
[60] *Id.* at 231.
[61] Brendan Z. Allison, Josef Faller & Christa Neuper, *BCIs That Use Steady-State Visual Evoked Potentials or Slow Cortical Potentials*, *in* BRAIN-COMPUTER INTERFACES: PRINCIPLES AND PRACTICE 241 (Jonathan Wolpaw & Elizabeth Winter Wolpaw eds., 2012). Certain SMR-BCIs may also work better than P300-based BCIs for "thought-to-text"

Steady-state visual evoked potentials (SSVEPs) appear 70 to 100 milliseconds after someone detects a repetitive visual stimulus, such as a flashing light.[62] SSVEP-based BCIs usually depend on the user's control of their gaze, so they do not work for people who have trouble moving their eyes.[63] For people who do have control of their gaze, SSVEP-based BCIs are straightforward to use—no need to imagine movement—but the flickering stimuli may be annoying.[64]

Error-related negative evoked potentials (ERNs) appear 50 to 200 milliseconds after someone detects that an event does not match what they intended to do.[65] ERNs are useful as secondary signals to help a BCI's algorithm correct problems when the user is not able to produce their desired outcome.[66]

3. Limits of Available Consumer BCI Technology

As mentioned above, the BCIs currently available to consumers are simple external BCIs.[67] By and large, they are sleek, futuristic-looking headbands that record EEG data much like a FitBit records your heart rate.[68] The functionality of these BCIs is limited by "internal" technological constraints, such as signal quality and user compatibility, and "external" constraints, such as the resource-intensive nature of BCI development and regulatory approval processes. There is also the ever-present risk that BCI development, regulation, and use will aggravate existing disparities, particularly those of race, gender, and ability. Conventional EEG electrodes, for example, do not work well with curly or tightly coiled hair, so researchers tend to exclude potential participants with those hair textures.[69] As a result, Black people are often underrepresented in EEG-based studies.[70]

---

applications because they are more amenable to multi-directional control, which lets users pick letters faster. *Id.* at 246.

[62] *Id.* at 241.

[63] *Id.* at 244.

[64] *Id.*

[65] Greenberg, *supra* note 53, at 86.

[66] *Id.* at 87.

[67] One can argue that some FDA-regulated implants are BCIs, but for the purposes of this comment I understand a consumer product to be one that can be purchased and used "off the shelf" without the need for a medical procedure.

[68] *See, e.g.*, MUSE, *supra* note 12.

[69] Tricia Choy, Elizabeth Baker & Katherine Stavropoulos, *Systemic Racism in EEG Research: Considerations and Potential Solutions*, 3 AFFECTIVE SCI. 14, 15 (2022).

[70] *Id.* at 15–16.

Of particular concern are the ways in which machine learning algorithms replicate biases, both explicit and implicit.[71] AI's bad track record with facial (non)recognition is just now entering public discourse.[72] But facial (non)recognition is just the tip of a large and dangerous iceberg. Even if developers managed to create a truly neutral algorithm, there is still the risk that the collection and aggregation of data allows a human to make biased decisions.[73] The replication of human biases is further explored in Part II of this comment; the rest of this section focuses on the other limitations mentioned above.

The most significant limit of currently available consumer BCIs may be better labeled as a misconception: They are not mind-reading devices. BCIs cannot tell you much about your brain. They can tell you even less about your mind.[74] Despite the proliferation of claims implying the contrary, most consumer BCIs do not employ research-grade EEG.[75] Even if they did, EEG is not a fine enough tool to probe the details of our thoughts with much accuracy outside of the well-controlled parameters of a research experiment.[76] While SMRs tell you that someone is moving a limb (or thinking about moving a limb), other signals such as the P300 reveal little without extra information about the stimuli that evoked them.[77] Studies

---

[71] Karl Manheim & Lyric Kaplan on AI and objectivity:

> Objectivity is not one of AI's virtues. Rather, algorithms reflect back the biases in the programming that are input when models are designed and in the data used to train them. Additionally, while data analysis can identify relationships between behaviors and other variables, relationships are not always indicative of causality. Therefore, some data analysis can develop imperfect information caused by algorithmic limitations or biased sampling. As a result, decisions made by AI may intensify rather than remove human biases contrary to popular conception. This poses real risks for equality and democracy.

Artificial Intelligence: Risks to Privacy and Democracy, YALE J.L. & TECH. 108, 158 (2019); Wolkenstein, Jox & Friedrich, *supra* note 38, at 637–39 (summarizing the major ethical issues that algorithm use poses, including a lack of transparency, mistaking correlation for causation, and both user- and tech-generated biases).

[72] *See generally* CODED BIAS (Shalini Kantayya 2020) ("When MIT Media Lab researcher Joy Buolamwini discovers that most facial-recognition software misidentifies women and darker-skinned faces, she delves into an investigation of widespread bias in algorithms.").

[73] CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION 15–31 (2016).

[74] In part because neuroscientists still are not sure about the relationship between the brain (the physical organ) and the mind (the concept of consciousness, identity, and those things that keep philosophers up at night).

[75] Iris Coates McCall & Anna Wexler, *Peering into the Mind? The Ethics of Consumer Neuromonitoring Devices*, in DEVELOPMENTS IN NEUROETHICS AND BIOETHICS 1, 5 (Vol. 3, 2020)

[76] *Id.* at 16.

[77] Francis X. Shen, *Neuroscience, Mental Privacy, and the Law*, 36 HARV. J.L. & PUB. POL'Y 653, 679–87 (2013).

demonstrating retrieval of personal information from a consumer BCI often involve looking at the raw EEG data alongside contextual information about the user's environment gathered from another source.[78] For a consumer P300- and ERN-based BCI to provide information about a user's responses to Facebook advertisements, for example, it would likely require some means of data sharing with Facebook or a supplementary mechanism that detected the content of the user's Facebook activity.[79] The need for supplementary information is a fact of life for the majority of BCIs currently in existence, both consumer and research. Kernel, a neurotechnology company launched in 2016, developed a BCI algorithm called "Sound ID" that can identify what song someone is listening to in under thirty seconds.[80] From one perspective, this is an extraordinary advance. For those worried about next-gen eavesdropping, however, take heart. The experiment that the Kernel team ran to test "Sound ID" only included ten songs.[81]

In addition to a lack of mind-reading powers, BCIs are also limited by the available mechanisms for picking up brain signals. External BCIs have a signal quality constraint—picking up brain signals through the skull is like listening to someone talking on the other side of a wall. Internal BCIs, meanwhile, can get up close and personal with the brain but are poor candidates for widespread consumer use. Although surgeons across the world insert cochlear implants and pacemakers every day, brain surgery carries a number of inherent risks. And as humankind has relatively little experience sticking hardware in people's brains, the long-term biocompatibility of internal BCIs is still an open question.[82] It may be physically infeasible to craft an internal BCI that needs minimal updates and lasts long enough to make the surgery worth it. Researchers have limited tools, as "wait and see" experiments are ethically impermissible. Private companies are not held to the same research ethics standards as academic institutions. One would

---

[78] Studies demonstrating remote "brain hacking" indicate that it is physically feasible. However, there is scholarly disagreement over the level of actual risk current technology poses. *Compare* Anna Wexler, *Separating Neuroethics from Neurohype*, 37 Nature Biotechnology 990 (2019), *with* Marcello Ienca & Pim Haselager, *Hacking the Brain: Brain-Computer Interfacing Technology and the Ethics of Neurosecurity*, 18 Ethics & Information Technology 117 (2016), *and* Marcello Ienca, Pim Haselager & Ezekiel J Emanuel, *Reply to "Separating Neuroethics from Neurohype,"* 37 NATURE BIOTECHNOLOGY 991 (2019).

[79] *See* Greenberg, *supra* note 53, at 94.

[80] Hello Humanity, KERNEL, https://www.kernel.com/hello-humanity.pdf#Experiments [https://perma.cc/8ZR7-9WL3].

[81] *Id.*

[82] *See, e.g.*, MONIKA GOSS-VARLEY, KEITH R. DONA, JUSTIN A. MCMAHON, ANDREW J. SHOFSTALL, EVON S. EREIFEJ, SYDNEY C. LINDNER & JEFREY R. CAPADONA, SCIENTIFIC REPORTS, MICROELECTRODE IMPLANTATION IN MOTOR CORTEX CAUSES FINE MOTOR DEFICIT: IMPLICATIONS ON POTENTIAL CONSIDERATIONS TO BRAIN COMPUTER INTERFACING AND HUMAN AUGMENTATION, at 2 (2017).

hope—perhaps in vain—that industry pressures and the threat of government action, if not a sense of moral opprobrium, would be enough to stop firms looking to cut corners.

To make things more difficult for BCIs, brain signals of the same general type differ between people and can even differ over time in the same individual.[83] This means that both the user and the BCI must be trained to "recognize" each other.[84] For many tasks, this training process requires a skilled technician to assist the user each time they connect to the BCI. Some BCIs may need regular calibrations to work properly—if they work at all.[85] One study found that roughly a fifth of people who tested SMR-based BCIs could not control them.[86] A greater percentage of testers across studies have successfully used P300- and SSVEP-based BCIs, but researchers are still trying to create a "universal" BCI.[87] Rather than fine-tune sensors that target one kind of signal, many researchers have instead tried to supplement them with additional sensors targeting other signals, both electric and non-electric.[88] While this effort has generated some success, the resulting BCIs are even more complex, which makes them more difficult to build, study, and use than BCIs that target one signal type.[89]

As the preceding paragraphs should make clear, BCI development and production is resource intensive. This need for resources is another limit on the availability of consumer BCI technology. External BCIs that allow users to interact with the world, rather than simply collect EEG data, require costly equipment. Internal BCI development poses substantial ethical and bioengineering challenges. Furthermore, private companies looking to get in the consumer BCI market early have to contend with the spectre of the Food and Drug Administration's costly premarket approval process.[90] Most investors are wary of putting money into the development of products that are unlikely to appear on shelves.[91]

FDA requires premarket approval for devices in "Class III," which covers devices "that support or sustain human life, are of substantial

---

[83] Inchul Choi, Ilsun Rhiu, Yushin Lee, Myung Hwan Yun, & Chang S. Nam, *A Systematic Review of Hybrid Brain-Computer Interfaces: Taxonomy and Usability Perspectives*, 12 PLOS ONE 2 (2017).
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] *Id.*
[88] *Id.*
[89] *Id.* at 2–3.
[90] *Premarket Approval: When a PMA is Required*, FOOD & DRUG ADMIN., https://www.fda.gov/medical-devices/premarket-submissions-selecting-and-preparing-correct-submission/premarket-approval-pma#when [https://perma.cc/TU7R-HKWU] (last updated May 16, 2019).
[91] *See* Wexler & Reiner, *supra* note 10, at 3.

importance in preventing impairment of human health, or which present a potential, unreasonable risk of illness or injury."[92] BCIs could conceivably fall under all three descriptions of Class III devices.[93] Companies can attempt to evade, and do evade, FDA's jurisdiction by claiming that a device supports wellness rather than health.[94] FDA's device regulation division, the Center for Devices and Radiological Health, issued a guidance document in 2016 that announced a decision not to examine "low risk general wellness devices."[95] This is no guarantee for would-be consumer BCI developers, however. Guidance documents are non-binding and can be changed without a public notice and comment process.[96] Even without a change, at least some external BCIs may not qualify as low risk. The relevant language in the 2016 guidance document is broad: If a device is invasive, or implanted, or "involve[s] an intervention or technology that may pose a risk to the safety of users and other persons if specific regulatory controls are not applied," the device is not low risk.[97] In addition, a low risk device cannot be similar to a device that FDA actively regulates.[98] Accordingly, FDA regulation of any particular BCI is far from a sure bet, FDA disinterest in BCIs is not a foregone conclusion, either.

B. Why Regulating BCIs is Challenging

1. The Pacing Problem

Government agencies often lack the resources and expertise necessary to keep up with BCIs and other rapidly developing technologies. When agencies do try to curb industry behavior, the resulting regulations can be

---

[92] *Premarket Approval: When a PMA is Required*, *supra* note 90.

[93] In May 2021, FDA released guidance on internal BCIs designed for patients with paralysis or amputated limbs. The document explicitly places "[n]on-implanted BCI devices" beyond its scope. FOOD & DRUG ADMIN., IMPLANTED BRAIN-COMPUTER INTERFACE (BCI) DEVICES FOR PATIENTS WITH PARALYSIS OR AMPUTATION—NON-CLINICAL TESTING AND CLINICAL CONSIDERATIONS 3 (2021) .

[94] *See* Wexler & Reiner, *supra* note 10, at 2.

[95] POLICY FOR LOW RISK DEVICES, *supra* note 17, at 2 ("CDRH does not intend to examine low risk general wellness products to determine whether they are devices within the meaning of the FD&C Act or, if they are devices, whether they comply with the premarket review and post-market regulatory requirements for devices under the FD&C Act . . . .").

[96] *Guidance Documents (Medical Devices and Radiation-Emitting Products)*, FOOD & DRUG ADMIN., https://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/guidance-documents-medical-devices-and-radiation-emitting-products [https://perma.cc/YCS4-KX89].

[97] POLICY FOR LOW RISK DEVICES, *supra* note 17, at 5.

[98] *Id.* at 5–6.

inflexible or simply ill-suited to the problem they are meant to address.[99] This is the so-called pacing problem: Technologies left unregulated can lead to concrete harms, yet regulation can lag behind innovation, hindering it.[100] For some policymakers and scholars, this lag is reason enough to avoid the pacing problem altogether. Instead, they propose, regulators (particularly government agencies) should leave companies alone until there is concrete evidence that a given technology is harmful.[101]

Theirs is an attractive proposal when a technology promises incredible benefits, as BCIs do. If companies lack the room to experiment, they may not develop life-changing devices for people with muscle control issues, lost limbs, or chronic health conditions. Because a single type of BCI could be put to many uses—a mobility tool for some people and entertainment for others, say—companies who are not cowed by the risks inherent in government regulatory pressure are likely to see BCIs as a solid investment. A BCI gaming controller could trend among able-bodied influencers *and* allow gamers with mobility challenges to play games that lack built-in accessibility options.[102] There are also more controversial benefits to delaying regulation of emerging technologies, such as unhindered market growth. [103] For those who argue that people are generally willing to trade their privacy for more personalized goods and services, the richer, larger datasets that minimally regulated technologies produce are a noteworthy benefit.[104]

There is a significant possibility that BCIs will go unregulated even with consensus that some regulation is necessary. As political scientists have chronicled since the dawn of that profession, even highly salient problems can go unaddressed.[105] This is not to say that government action is a cure-all.

---

[99]Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, RICHMOND L.J. & TECH 2–3 (2015) (observing that regulation of emergent technology "is likely to be premature and overly rigid" and proposing that Internet of Things devices should not be subjected to "prophylactic restrictions" absent "clear evidence of direct risk to health or property").

[100] *See* Araz Taeihagh, M. Ramesh & Michael Howlett, *Assessing the Regulatory Challenges of Emerging Disruptive Technologies*, 15 REGUL. & GOVERNANCE 1009, 1009 (2021).

[101] *See, e.g.*, Thierer, *supra* note 99.

[102] *See* Antonio Regalado, *supra* note 7; *see also Our Work*, ABLEGAMERS, https://ablegamers.org/our-work/ [https://perma.cc/WGW9-DEAX] (last visited Feb. 6, 2022) ("We work within the industry to enable developers to create adaptive gaming solutions, design more inclusive games, and create events that are accessible to people with disabilities.").

[103] *See* Thierer, *supra* note 99, at 14.

[104] *Id.* at 57.

[105] There are multiple theories that attempt to explain this phenomenon. *See generally* TANYA HEIKKILA & PAUL CAIRNEY, COMPARISON OF THEORIES OF THE POLICY PROCESS, THEORIES OF THE POLICY PROCESS (Christopher M. Weible & Paul A. Sabatier eds., 4th ed. 2018).

The Toxic Substances Control Act of 1976[106] prevented the U.S. Environmental Protection Agency (EPA) from regulating most commercial chemicals for decades.[107] Although the 2016 Frank R. Lautenberg Chemical Safety for the 21st Century Act[108] overhauled the law, the EPA now has a huge backlog of chemicals to test.[109] Even if Congress and an agency are not at cross-purposes, the very structure of federal agencies could get in the way of regulatory efforts. It is not entirely clear, for example, which agency should take the lead on regulating consumer neurotechnology.[110]

I do not dispute that regulation should be targeted to specific problems that emergent technology poses.[111] Few would contend that general regulations that blanket everything and everyone without recourse to any cost-benefit analysis are a worthwhile endeavor. I do, however, suggest that waiting until concrete harms appear is not a great answer to the pacing problem in the context of especially high-potential, high-risk technologies such as BCIs.

Social media is a clear example of a disruptive technology left largely unregulated until it matured into a ubiquitous presence in most people's lives.[112] Reasonable people may disagree on whether individual social media users or "Twitter mobs" indicate a market failure. What is unsettling to many, I gather, is that the self-regulation of the industry's early days now takes the form of a handful of massive companies calling the shots. For some, this state

---

[106] *Summary of the Toxic Substances Control Act*, EPA, https://www.epa.gov/laws-regulations/summary-toxic-substances-control-act [https://perma.cc/JX2F-S3R2] (last updated June 2016).

[107] Mark Scialla, *It Could Take Centuries for EPA to Test All The Unregulated Chemicals Under a New Landmark Bill*, PBS NEWS HOUR (June 22, 2016, 11:58 AM EST) https://www.pbs.org/newshour/science/it-could-take-centuries-for-epa-to-test-all-the-unregulated-chemicals-under-a-new-landmark-bill [https://perma.cc/UJA4-KAJA].

[108] Frank R. Lautenberg Chemical Safety for the 21st Century Act, Pub. L. No. 114–128, 130 Stat. 448–513 (2016).

[109] Scialla, *supra* note 107.

[110] *See* Taeihagh, Ramesh & Howlett, *supra* note 100, at 1009.

[111] *See* Thierer, *supra* note 99, at 2–3:

> The better alternative to top-down regulation is to deal with concerns creatively as they develop, using a combination of educational efforts, technological empowerment tools, social norms, public and watchdog pressure, industry best practices and self-regulation, transparency, and targeted enforcement of existing legal standards (especially torts), as needed" but noting that "if enough people are attempting to modify their bodies or enhance various human capabilities, it may become very difficult for the law to keep up.

[112] Jack M. Balkin, *How to Regulate (and Not Regulate) Social Media*, Knight First Amendment Institute at 2 (Mar. 25, 2020), https://knightcolumbia.org/content/how-to-regulate-and-not-regulate-social-media [https://perma.cc/B94D-PYSM].

of affairs is nothing less than dire threat to democratic institutions.[113] Even if you dispute such a conclusion, it seems fair to say that regulators are struggling mightily to bring the social media giants to heel after letting them run free for years.[114]

Consumer BCIs might not be the next technology to fundamentally change how we interact with one another and how we see ourselves, but the curious evolution of social media indicates that waiting to regulate would be a great risk.[115] None of this is to say that BCIs are doomed to bring us all pain and turn us into a ruin of a species that will serve as a warning to all who might bring their spaceships close to the perpetually smoldering rock that used to be Earth. (Though that is always a possibility.) Regulation can be appropriate when technology presents a direct risk to a subset of humanity rather than the entire planet.

Even if BCIs fail to follow social media as an era-defining technology, regulation may be needed to avoid deepening existing inequities. The "emerging technology narrative" envisions all of society changing, all at once. Yet many technological advances reach the wealthy long before marginalized communities. Developers of consumer technologies often target privileged populations when making design, infrastructure, and marketing decisions. [116] In this way products which may have had widespread utility are rendered largely inaccessible to people who are not a member of a privileged population.[117]

Technology like the IpsiHand or a thought-to-text software could mean a lot to someone who seeks more control over how they interact with their environment. Such devices should not be available only to those who can afford to pay astronomical sums. Similarly, companies may treat "disabled" people only as potential customers rather than collaborators. Devices devised by the "able-bodied" may not meet the actual needs and

---

[113] Manheim & Kaplan, *supra* note 71, at 110–11 (warning that tech CEOs seem to have more power over American lives than elected representatives and that AI-powered software gives technology companies the ability to undermine or even displace government regulation).

[114] *See, e.g.*, Bobby Allyn, *Judge Allows Federal Trade Commission's Latest Suit Against Facebook to Move Forward*, NPR (Jan. 11, 2022, 5:10 PM ET), https://www.npr.org/2022/01/11/1072169787/judge-allows-federal-trade-commissions-latest-suit-against-facebook-to-move-forw [https://perma.cc/PY6A-89XB].

[115] *See* Balkin, *supra* note 112, at 9.

[116] *See* Courtney R. Lyles, Robert M. Wachter & Urmimala Sarkar, *Focusing on Digital Health Equity*, 326 JAMA 1795, 1795 (2021) (arguing that digital health tools are deepening health inequities because they "are developed with homogeneous, highly educated, and advantaged populations in mind").

[117] *Id.* ("despite the ability to leverage technology to design apps in multiple languages or with audiovisual features to support both personalization and accessibility, most available digital health tools are available in English only and are written at high reading levels").

wants of their intended users. People may not wish to change themselves in order to realize a range of mobility, mental capacity, or mode of communication labeled "normal."[118] Early regulatory intervention—government or industry—could prevent such exclusionary feedback loops and encourage more equitable innovation.[119]

2. The Internet of Things Requires New Approaches to Data Protection

Targeted, early regulatory intervention of BCIs may sound like a tall order with little chance of being filled. But BCI regulation need not be BCI specific. Currently available consumer BCIs may offer unique benefits, but their risks are largely the same as other Internet of Things (IoT) and AI devices. Of course, this does not mean that regulating IoT and AI devices as a group is any more straightforward than regulating BCIs in particular.

Many IoT and AI devices present data privacy risks. Consequently, they trigger the pacing problem—regulate now, and potentially stifle innovation, or regulate later, potentially violating strongly held societal privacy norms?[120]

Like social media, the Internet of Things has been described as another tech advance that proliferated before any serious regulatory efforts.[121] Wearable technology and now-familiar home assistants such as Alexa collect amounts of data that could be orders of magnitude beyond what consumers

---

[118] See *Community and Culture—Frequently Asked Questions*, NAT'L ASSOC. DEAF:

> The deaf and hard of hearing community is diverse. There are variations in how a person becomes deaf or hard of hearing, level of hearing, age of onset, educational background, communication methods, and cultural identity. How people "label" or identify themselves is personal and may reflect identification with the deaf and hard of hearing community, the degree to which they can hear, or the relative age of onset.

https://www.nad.org/resources/american-sign-language/community-and-culture-frequently-asked-questions/ [https://perma.cc/2LRA-M62Y] (last visited Feb. 6, 2022).

[119] Lyles et. al, *supra* note 116, at 1796 ("Building and testing tools in the populations who need and can benefit from them offer the best opportunity to ensure that the health care digital revolution improves health equity. Also needed is intentional implementation that carefully leverages in-person support and builds from trusted relationships.")

[120] For a fuller discussion of privacy law and theories, see subsection 3, How the "Privacy Narrative" Influences BCI Risk Assessment, *infra.*

[121] *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 92 (2014) ("[IoT devices] are not a science-fiction future but a present reality. Internet of Things devices have proliferated before we have had a chance to consider whether and how best to regulate them.").

believe they are sharing.[122] Some consumer BCIs produce data that provide minimal information about who their users are, their preferences, or their health. But data that reveals little on its own can, when combined with other data, give rise to accurate inferences (or inaccurate, biased ones) about sensitive information that most people would think twice before sharing.[123] Taken together, consumer IoT devices are part of an impossibly massive and impossibly rich dataset.[124]

IoT is not a definition so much as a shorthand reference for a big group of devices (things) that share one basic characteristic: access to the internet.[125] With few, if any, exceptions, consumer BCIs share brain data over the internet with other devices or cloud storage servers.[126] Muse, a "mediation headband" with EEG functionality, works with a smartphone app that gives users "real-time feedback" by playing different weather sounds depending on their "mental state."[127] The team behind the now defunct Melon, another consumer EEG headband company, promised that the Melon device would "improve your focus in relation to your activity, your environment, your emotions, and any other behavior you want to track."[128] And with few, if any, exceptions, both consumer and research BCIs use AI to translate brain signals into outputs like moving a computer cursor.[129]

There is also emerging evidence that most methods of anonymizing and pseudonymizing data can be reversed.[130] Some scholars predict a world

---

[122] Jane Kirtley & Scott Memmel, *Rewriting the "Book of the Machine": Regulatory and Liability Issues for the Internet of Things*, 19 MINN. J.L. SCI. & TECH. 455, 466 (2018) (noting that IoT devices collect various kinds of sensitive data, including health data, and aggregate it, creating exceptionally rich data sets).
[123] *Id.*
[124] Peppet, *supra* note 121.
[125] *Id.* at 92.
[126] Marcello Ienca, Pim Haselager & Ezekiel J Emanuel, *supra* note 16.
[127] MUSE, *supra* note 12.
[128] Melon: A Headband and Mobile App to Measure Your Focus, KICKSTARTER, https://www.kickstarter.com/projects/806146824/melon-a-headband-and-mobile-app-to-measure-your-fo [https://perma.cc/B2LP-NT85] (last visited Jan. 20, 2022). Melon is no longer available.
[129] Wolkenstein, Jox & Friedrich, *supra* note 38, at 639.
[130] Peppet, *supra* note 121, at 98 (health), 100 (wearable sensors), 102 ("epidermal electronics"), 103 (implantables), 108 (smart home), 111 (employee sensors), 115 (smartphone sensors—mood sensing). Without mentioning BCIs as a category, Peppet does list the Melon and Muse headsets as examples of IoT devices and the potential ability of smartphone sensors to pick up information about the user's mood and health. *Id.* at 88 n.11. *See also* Michelle M. Christovich, *Why Should We Care What Fitbit Shares?: A Proposed Statutory Solution to Protect Sensitive Personal Fitness Information*, 38 HASTINGS COMMC'N & ENT. L.J. 91, 109–10 (2015) (discussing wearable fitness tracker manufacturers' privacy policies with regard to identifying data).

where employers use the data from wearables to monitor their employees.[131] This could turn wearable manufacturers into de facto credit reporting agencies, which would bring them within the ambit of the Fair Credit Reporting Act.[132]

Currently, regulatory efforts to control both legal and illegal forms of data collection and sharing tend to focus on protecting personal information. A conventional mode of protecting personal information rests on the idea of voluntary informed consent.[133] As we generate increasing amounts of data across an expanding number of devices, however, truly informed and voluntary consent has become nearly impossible to achieve. When was the last time you read through a privacy policy or end user license agreement before clicking or tapping "agree"?[134] There is often little reason to spend the time, as declining the terms and conditions means that you cannot use the product that you just bought. [135] To make matters more complex, few

---

[131] Peppet, *supra* note 121, at 127– 28; Alexandre Gonfalonieri, *What Brain-Computer Interfaces Could Mean for the Future of Work*, HARV. BUS. REV. (Oct. 6, 2020), https://hbr.org/2020/10/what-brain-computer-interfaces-could-mean-for-the-future-of-work [https://perma.cc/4QQM-F6GA].

[132] Peppet, *supra* note 121, at 126–27:

> The FTC has warned mobile-application developers that if they provide information to employers about an individual's criminal history, for example, they may be providing consumer reports and thus regulated by the FCRA. By analogy, if a consumer sensor company such as Fitbit began to sell their data to prospective employers or insurance companies, the FTC could take the position that Fitbit had become a CRA [(consumer reporting agency)] under the FCRA. If a company such as Fitbit were classified as a CRA, consumers would have the right to dispute the accuracy of any information provided by such a CRA. If Internet of Things manufacturers were not deemed CRAs, but instead deemed to be providing information to CRAs—such as established credit-reporting firms or data aggregators—the FCRA would forbid Internet of Things firms from knowingly reporting inaccurate information and would require that such firms correct and update incomplete or incorrect information.

[133] Anita L. Allen, *An Ethical Duty to Protect One's Own Informational Privacy?* 64 ALA. L. REV. 845, 847, 856 (2013) (discussing the modern approach to digital information sharing as "great privacy give-away" and offering the possibility that protecting one's own informational privacy is a self-regarding duty).

[134] Marcus Moretti & Michael Naughton, *Why Privacy Policies Are So Inscrutable*, THE ATLANTIC (Sept. 5, 2014), https://www.theatlantic.com/technology/archive/2014/09/why-privacy-policies-are-so-inscrutable/379615/ [https://perma.cc/N2HW-MZUV] (suggesting that even if consumers wanted to read through all of those privacy policies, they likely wouldn't have the time).

[135] Graham Johnson, *Privacy and the Internet of Things: Why Changing Expectations Demand Heightened Standards*, 11 WASH. U. JURIS. REV. 345, 354 (2019) (discussing end user adhesion contracts for IoT products: "[C]onsumers are presented with a 'choice,' but that choice is little more than the manufacturer stating 'take it or leave it'—either accept the terms of use, or don't use the product.")

wearables have screens large enough to allow the user to read the monstrously large walls of text that make up modern privacy policies.[136] The privacy-minded consumer must navigate to a webpage or link the IoT device to an app on a smartphone or computer if they want to read that wall of text.[137]

These issues with a consent-based approach to protecting personal information may not mean much for future regulatory efforts that encompass BCIs. Some scholars contend that most consumers do voluntarily consent to companies using and sharing their data.[138] After all, many people post intimate details about their lives on the internet and purchase devices with the express purpose of generating data about themselves.[139]

Other scholars reply, however, that most consent is inadequate because few companies tell consumers much about their data collection, storage, and sharing policies.[140] Even if the majority of consumers make decisions that they believe are in line with their perceived interests, they may have decided to share much less if they were aware of what was really being shared.

Companies can, of course, require consumers to waive the rights to their data by including a clause to that effect in the terms and conditions that accompany their product or service. But the notion that a company can do whatever it pleases with information it gathers from consumers, potentially without their knowledge or express consent, is intuitively suspect. This is especially so when the data is generated as a side effect of the consumer's use of the product or service, such as EEG data generated by a BCI headband. If we have no choice but to allow companies to collect data about us—data that might reveal personal information—can it be right that we have no say in how that data is used or stored? It is difficult to argue that consumers are *forced*, in the strict sense of the term, to use IoT devices. There are plenty of devices on the market, BCIs among them, that are unnecessary. Yet few of us could get by without a phone or a computer, as most employers require employees to be available via phone, email, or both. Many workplaces rely

---

[136] Moretti & Naughton, *supra* note 129.

[137] Peppet, *supra* note 121, at 141 (surveying various IoT products' privacy policies).

[138] Thierer, *supra* note 99, at 68 (contending that privacy is subjective and noting that people routinely share personal information about themselves, suggesting that they have decided that the benefits of doing so outweigh the costs).

[139] *Id.; see also* Anita L. Allen, *Dredging Up the Past: Lifelogging, Memory, and Surveillance*, 75 U. CHI. L. REV. 47, 52 (2008) ("Why would anyone want to make a multimedia record of her entire life? The answer may be that our experiences and achievements comprise our uniqueness; preserving a record of them preserves a record of us.").

[140] Thierer, *supra* note 99, at 68; Christovich, *supra* note 130, at 105. *See also* Manheim & Kaplan, *supra* note 71, at 131–33 (working from the assumption that privacy contributes to the maintenance of strong democratic institutions, arguing that consumers have acquiesced to privacy invasions because they feel that they lack control over their data).

on remote work applications such as Microsoft Teams and G Suite or electronic employee management systems. One can argue that technology companies do give consumers *some* control over what is done with data that contains their personal information with, for example, those cookie alert menus.[141] For complex IoT devices such as BCIs, however, the data may be difficult for most consumers to interpret.[142] Accordingly, issues with a consent-based approach to protecting personal information actually mean a great deal for future regulatory efforts that encompass BCIs.

One approach to the intertwined issues of consent and ownership is for data subjects to have complete control over any data that includes information about them. This would mean that companies would have to ask consumers for their data, not simply for their consent. The practical challenges with such an approach to consumer data are easy to see. Even if there were a simple way to automatically transfer data from corporate cloud servers, cell sites, and the like, it would be nearly impossible for most people to store even a fraction of the data their IoT devices generate. Then there is medical data, surveillance camera footage, and all of the other data that non-consumer IoT devices generate. Who would have the time (or knowledge) to manage all of that? The privacy policies and terms and conditions agreements we are all familiar with could reemerge in short order. If legal control passed to consumers, but not actual control of the data, enforcement would be nearly impossible. Consumers would have little incentive to press isolated incidents of impermissible data usage, if they were even aware of them, but companies would have strong incentives to devise artful means of securing access to as much data as possible.

Still, this approach could be effective in limited circumstances. Some Indigenous scholars and activists have advocated data sovereignty—the transfer of legal ownership and control of all Indigenous data to Native nations.[143] Acknowledging the practical difficulties, they argue that the call

---

[141] *See* Emily Stewart, *Why Every Website Wants You to Accept Its Cookies*, VOX: RECODE (Dec. 10, 2019, 8:00 AM EST), https://www.vox.com/recode/2019/12/10/18656519/what-are-cookies-website-tracking-gdpr-privacy [https://perma.cc/4MAD-6BKL].

[142] *See* Anastasia Greenberg, *supra* note 53, at 109:

> In a BMI with 24 channels and with a sampling rate (i.e., rate of data collection) of 200 Hz, there will be over 17 million data points for just one hour of BMI use. In that case, if a data subject requests access to their brain data, not only will it be practically impossible for an ordinary individual to make any sense of the information, they will unlikely have the disk space on their computer to download the data in the first place.

[143] *About Us*, UNITED STATES INDIGENOUS DATA SOVEREIGNTY NETWORK, https://usindigenousdata.org/about-us [https://perma.cc/E99B-HHZ6] (last visited Feb. 6, 2022) ("Indigenous data sovereignty is the right of a nation to govern the collection, ownership, and application of its own data. It derives from tribes' inherent right to govern

for data sovereignty follows naturally from their enduring struggle to restore land and resources to Indigenous governance.[144] For these scholars and activists, data is not merely inert property but a vessel of cultural and biological knowledge; it is *of* them, rather than *about* them.[145]

3. How the "Privacy Narrative" Influences BCI Risk Assessment

The variety of relationships we humans have with the data we generate makes the question of managing privacy risks difficult. Above, I discussed how consumer BCIs cannot do much more "mind-reading" than a mood ring. Even with this information, it can be difficult to stop thinking about the monkey playing Pong, a commercially available thought-to-text device, and people spying on the innermost workings of your mind (as you think about the monkey). For his part, Musk has suggested that Neuralink may one day make human-AI symbiosis possible.[146] For many people, especially those familiar with the Borg from *Star Trek*, the idea of merging humans and AI may be startling and scary. Even if you are the type of science fiction fan who likes the idea of becoming a human-AI hybrid, you might have a few questions about how it would actually work. When it comes to technology, humans tend to focus on the dramatic unknown. This focus can get in the way of regulation that effectively balances both innovation and risk management concerns.

Assessing competing risks can be tricky. When a grave harm is likely to occur, it makes sense to ignore other, smaller risks and devote attention to that grave harm. If you were to spot a wildfire off in the distance that was threatening to consume your home, chances are good that you would want to prepare for that fire rather than fix a leaky faucet. (No home, no faucet to fix.) Even when a grave harm is unlikely, taking precautions against that grave harm can feel more important than addressing a more likely, but relatively minor, harm. Even if you were not sure that your home was in the path of the fire, or that what you were looking at was even a fire, you might spend time thinking about what you would do in the event of a fire instead of fixing the leaky faucet.

---

their peoples, lands, and resources. This conception of data sovereignty positions Indigenous nations' activities to govern data within an Indigenous rights framework.").

[144] *Id.*

[145] *Id.*

[146] Nicole Wetsman, *Elon Musk Trots Out Pigs in Demo of Neuralink Brain Implants*, THE VERGE (Aug. 28, 2020, 7:45 PM EDT), https://www.theverge.com/2020/8/28/21406143/elon-musk-neuralink-ai-pigs-demo-brain-computer-interface [https://perma.cc/HWZ4-NS62].

Misleading advertising can harm BCI consumers.[147] Like a leaky faucet, which wastes water and could invite mold, it is a current problem with clear harms. But more than a few BCI observers are warning of wildfire. The media is full of recitations of Musk's plans for Neuralink (like the one at the beginning of this comment)[148] and pieces with titles such as "The Brain Implants That Could Change Humanity."[149] A common refrain: *Will my thoughts stay my own?*[150] Early in 2021, ScienceNews asked its readers whether they were concerned about how advances in neurotechnology might affect them.[151] Far and away, readers were worried about their privacy—both their ability to control who accesses information about themselves and their ability to make their own choices. One wrote ScienceNews that the idea of someone remotely accessing a person's brain was "absolutely terrifying"; another said that they had "no wish/desire to become a zombie or a clone."[152] Sensationalist? Maybe. Yet some neuroscientists, neuroethicists, and neurolawyers (yes, they exist) have also expressed concerns about letting this technology develop without clear boundaries to protect users' privacy.[153] This mix of worries and questions—some fanciful, some pragmatic---can be understood as a "privacy narrative." Managing this narrative is perhaps the most pressing challenge of BCI regulation at this stage of the technology's development. It is difficult to prepare for a fire if you do not know its velocity or size—or whether it is on the horizon at all.

I now turn to a brief discussion of privacy law and theories to shed light on the shape of the privacy narrative. The existence of a legal right to privacy, whatever "privacy" means in practice, is well settled in the United States. Since the middle of the 20th century, the Court has incorporated most of the Bill of Rights into the due process clause of Fourteenth Amendment. Before incorporation, no part of the Bill of Rights was enforceable against

---

[147] Anna Wexler & Robert Thibault, *supra* note 13.

[148] Scott Jung, *Elon Musk's Neuralink Shares More Abouts Its Implantable Brain Stimulator*, MEDGADGET (Aug. 31, 2020), https://www.medgadget.com/2020/08/elon-musks-neuralink-shares-more-about-its-implantable-brain-device.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Medgadget+%28Medgadget%29 [https://perma.cc/WH8T-CEVN]. Note that this piece calls Neuralink a "brain stimulator," not a brain-computer interface.

[149] Velasquez-Manoff, *supra* note 15.

[150] *See id.* The article's tagline ends with the phrase "are our daydreams safe?"

[151] Laura Sanders, *Can Privacy Coexist with Technology That Reads and Changes Brain Activity?*, SCIENCENEWS (Feb. 11, 2021, 6:00 AM).

[152] *Id.*

[153] *See, e.g.*, Sasha Burwell, Matthew Sample & Eric Racine, *Ethical Aspects of Brain Computer Interfaces: A Scoping Review*, 18 BMC MED. ETHICS 60, 61 (2017); Shen, *supra* note 77.

the states—it only bound the federal government.[154] The Court has also made use of the controversial notion of substantive due process to protect other fundamental rights that are not expressly mentioned in the Bill of Rights through the Fourteenth Amendment's due process clause.[155] For a time, substantive due process was explained in terms of privacy.[156] In *Griswold v. Connecticut*, Justice Douglas reasoned that the Constitution protected an unenumerated right to privacy on the ground that such a right fell within the overlapping "penumbras" of certain enumerated rights.[157] Although the Court has since moved away from the idea that the unenumerated rights that the Constitution protects emanate from the right of privacy, the existence of a constitutionally protected right to privacy has rarely been seriously questioned.

The content of that right is subject to near-constant questioning. The United States is home to many and sundry definitions of privacy, some of which overlap. The sources of privacy law also overlap—but only to a degree. Privacy, in its multiple forms, is protected by various parts of the United States Constitution, federal and state statutes, federal and state regulation, and various industry standards, both binding and voluntary. Some of these sources of law bind the government, some bind private actors, and some bind both.

Some statutes and regulations limit certain third parties from sharing information we, willingly or unwillingly, share with them. Despite efforts both within and without Congress, there is no federal statute that protects individuals' privacy across the board. Instead, there are a series of industry-specific statutes, such as the Health Insurance Portability and Accountability Act (HIPAA).[158] In addition, a handful of states have more comprehensive

---

[154] *See* Mapp v. Ohio, 367 U.S. 643, 655–66 (1961) (overturning precedent by holding that Fourth Amendment protections are enforceable against the states through the due process clause of the Fourteenth Amendment).

[155] Some have argued that Substantive Due Process, even if justified by the structure of the Constitution and precedent, is a dangerous doctrine because it invites the Justices to go on fishing expeditions to find unenumerated rights in the constitution that match their own beliefs and policy preferences. This argument is a particularly common rejoinder to *Roe v. Wade*, *Casey v. Planned Parenthood*, and *Hobby Lobby*. *See* Nathan S. Chapman & Kenji Yoshino, *Common Interpretation: The Fourteenth Amendment Due Process Clause*, NAT'L CONST. CTR., https://constitutioncenter.org/interactive-constitution/interpretation/amendment-xiv/clauses/701 [https://perma.cc/FG7D-H66D] (last visited Feb. 6, 2022) (elucidating the controversy around substantive due process in light of the Supreme Court's history).

[156] Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

[157] Chapman & Yoshino, *supra* note 155.

[158] *The HIPAA Privacy Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html [https://perma.cc/E6X7-8BGN] (last updated December 7, 2021); *see also Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, CDC, https://www.cdc.gov/

privacy statutes. The Federal Trade Commission (FTC) also protects consumer privacy insofar as disclosures of personal information are the result of unfair or deceptive trade practices.[159] FTC enforcement actions for Internet of Things (IoT) security breaches demonstrate that the FTC could mount similar actions against BCI manufacturers without changing its approach.[160]

As discussed above, IoT devices put pressure on traditional notions of personal information, voluntary consent, and ownership.[161] There is an emerging consensus that existing privacy law is unsuited for the complexities of modern data, particularly the growth of IoT and AI technologies. Since BCIs are part of the larger categories of IoT and AI, they inspire many of the same privacy concerns as more familiar technologies, such as Alexa.[162] As noted privacy scholar Anita Allen has argued, the advent of the digital age brought a torrent of tricky privacy issues.[163] Do we have an ethical duty to protect our own privacy?[164] If so, how can we protect our privacy in a "Big Data economy?"[165]

Adding thoughts to the mix seems to make tricky privacy issue trickier. Nita Farahany has written extensively on the potential challenges of squaring the Fourth and Fifth Amendments of the U.S. Constitution, among other sources of law, with potential future technologies that render thoughts and involuntary mental processes accessible to others.[166] Some neuroethicists, meanwhile, have argued that products already available to consumers present clear privacy risks because they are at once rich sources of personal information and vulnerable to "brain hacking."[167]

---

phlp/publications/topic/hipaa.html#one [https://perma.cc/JSG5-FZH7] (last updated Sept. 14, 2018) ("(HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.").

159 *See Business Guidance: Privacy and Security*, FTC, https://www.ftc.gov/tips-advice/business-center/privacy-and-security [https://perma.cc/A4ZM-DD7F] (last visited Feb. 6, 2022) (offering advice for business owners to help them meet their legal obligations regarding consumer privacy and avoid FTC enforcement actions).

160 Kirtley & Memmel, *supra* note 122, at 473-81.

161 Anastasia Greenberg, *supra* note 53, at 94 (classifying consumer BCIs as IoT devices).

162 *See generally,* Anne Pfeifle, Comment, *Alexa, What Should We Do About Privacy? Protecting Privacy for Users of Voice-Activated Devices*, 93 WASH. L. REV. 421 (2018) (examining privacy considerations by highlighting the use of Amazon's Alexa device).

163 *See generally* Anita L Allen, *Protecting One's Own Privacy in a Big Data Economy,* 130 HARV. L. REV. FORUM 71 (2016) (linking issues of individual privacy and responsibility to participation in a modern socio-economy).

164 Allen, *supra* note 133.

165 Allen, *supra* note 163.

166 *See, e.g.*, Nita A. Farahany, *Incriminating Thoughts*, 64 STAN L. REV. 351 (2012); Nita A. Farahany, *The Costs of Changing Our Minds*, 69 EMORY L. J. 75 (2019). For an excellent summary of Farahany's work and comparisons with other scholars, circa 2013, *see* Shen, *supra* note 77.

167 Burwell, Sample & Racine, *supra* note 153.

"Thought privacy" is not as novel an idea as it sounds. It is not limited to fiction, either. In the 1928 U.S. Supreme Court case *Olmstead v. United States*, Chief Justice Taft held that a particular instance of government wiretapping did not violate the Fourth Amendment because the government agents in question did not physically trespass on the petitioners' property but merely recorded a conversation, from a distance, into which the petitioner voluntarily entered.[168] Justice Brandeis dissented, returning to an argument that he and Samuel Warren made in their famous 1890 article *The Right to Privacy.*[169] Urging the majority to consider the future effect of their holding, he warned:

> The progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. *Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions*. . . . Can it be that the Constitution affords no protection against such invasions of individual security?[170]

In *The Right to Privacy*, Justice Brandeis and Warren argued for the existence of a right, found in the common law rather than the Constitution, "of determining, ordinarily, to what extent [one's] thoughts, sentiments, and emotions shall be communicated to others."[171]

Such concerns fall into the "informational privacy" category.[172] They focus on thoughts as a type of data that can be collected, analyzed, transferred, and stored.[173] Connecting brains and computers has given rise to another category of privacy concerns, however. It is possible to understand thoughts as more than something we "own" or can exercise control over, like other kinds of data. Our thoughts are also part of us. They play a large role in how we perceive our own consciousness and interpret reality. A device that "writes," or makes changes to, the brain may qualify as interference with

---

[168] Olmstead v. United States, 277 U.S. 438 (1928).
[169] *Id. See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. R. 193 (1890).
[170] *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting) (emphasis added).
[171] Warren & Brandeis, *supra* note 169, at 198.
[172] *See* Jeroen van den Hoven, Martijn Blaauw, Wolter Pieters & Martijn Warnier, *Privacy and Information Technology*, *STAN. ENCYCLOPEDIA PHIL.* (Edward N. Zalta , ed.) https://plato.stanford.edu/archives/sum2020/entries/it-privacy/ [https://perma.cc/94ZZ-VMW3] (describing informational privacy as "the interest of individuals in exercising control over access to information about themselves").
[173] *Id.*

"decisional privacy."[174] So too may a device that only "reads" the brain but uses AI to do so.[175] Complex AI algorithms employ predictive decision-making that humans usually cannot track.[176] If a device has multiple intricate functions, it may be difficult to tell whether the user is directing the AI or whether the AI is directing the user.[177]

The concept of decisional privacy, present in U.S. Supreme Court cases such as *Griswold v. Connecticut*, lacks a consistent scope and definition. In general, it covers the notion that there are certain decisions that individuals should be able to make for themselves without interference.[178] Another possible label for decisional privacy is "autonomy," though that term is also difficult to pin down.[179]

These queries about how machines that connect brains to computers may challenge established boundaries of informational and decisional privacy form a powerful, urgent narrative. Accessing thoughts seems to be a major threshold in human development. Even though the technology is still in its early stages, the stakes feel high and personal. Haven't we seen this play out in countless novels, movies, and video games? Technology that becomes sentient and turns on humanity—or makes us turn on our friends and family?

Some (likely many) people may be unwilling to ride the hype train that far. Even in the likely event that society does *not* descend into chaos caused by sentient implants or cyborgs, the ability to peer into someone's thoughts does seem poised to change how we interact with one another in profound ways, as social media did. The potentially transformative effects of this technology—though people will certainly disagree on what exactly those effects might be—keeps the "privacy narrative" relevant. Brain-computer communication may end up in history's dustbin alongside flying cars. But for now, the technology will continue to inspire reflection and action in people who have concluded, whether based on critically analyzed facts or gut instinct, that this technology really is the future. If some of those people are

---

174 *See generally* Drew, *supra* note 28, (noting ethicists' concerns about these technologies' interference with users' privacy and agency).

175 *Id.*

176 Wolkenstein, Jox & Friedrich, *supra* note 38, at 637-38.

177 Drew, *supra* note 28, at S20–S21.

178 Van den Hoven, Blaauw, Pieters & Warnier, *supra* note 172 (describing decisional or constitutional privacy as "the freedom to make one's own decisions without interference by others in regard to matters seen as intimate and personal . . . .").

179 *See generally* John Christman, *Autonomy in Moral and Political Philosophy*, THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Edward N. Zalta, ed.), https://plato.stanford.edu/archives/fall2020/entries/autonomy-moral/ [https://perma.cc/3K4N-VPF4] ("The variety of contexts in which the concept of autonomy functions has suggested to many that there are simply a number of different conceptions, and that the word simply refers to different elements in each of those contexts.").

regulators, they are going to have sort out which risks are worth addressing and which are too distant to be worth expending time and money on.

Sorting through these potential risks may be a Sisyphean task. Because the technology is still developing, there is not much empirical data that clearly supports conclusions about which privacy risks are realistic in the short term, which are realistic in the long term, and which are confined to the worlds of science fiction. In addition, many concerns are informed by normative judgments about the proper role of technology in society and the importance of distributing technological benefits and harms equitably. It may be reasonable to assume that many people would not like Elon Musk alone to decide how humanity should advance—even if they share in his desire to one day achieve human-AI symbiosis. But the hyper-polarization that typifies current politics, coupled with widespread distrust of expertise, strongly suggest that consensus on the best way forward will be monstrously hard to achieve. And even if the elected officials of the United States were able to reach consensus, or at least a workable compromise, those who hold only a small share of global power, both within and without the United States, would likely find themselves left out of the conversation. Truly "effective" regulation, I suggest, must attempt to address these moral and ethical challenges.

With that in mind, it is still possible to consider the interplay between the privacy narrative and the existing regulatory models. An outsize focus on the privacy narrative would probably lead to inefficient, wasteful regulation. BCIs have only just started leave research labs. In addition, the narrative incorporates a very broad definition of privacy that encompasses concrete worries about data protection (informational privacy) as well as concerns, which are potentially more intangible, about autonomy and identity (decisional privacy). It also overshadows leaky faucet issues with consumer product safety and marketing, which could be left unaddressed.[180] Francis Shen, using the term "mental privacy panic" to refer to the same general concept I call the "privacy narrative," cautions those who would let mind-reading fears influence policymaking.[181] The problem is not what current neuroscience technologies can do, he contends, but how various actors can "(mis)use[] and (mis)interpret[]" brain data.[182]

Yet ignoring the narrative entirely could lead to regulation that fails to take into account the ways in which that narrative impacts how people will interact with BCIs. The near-future development trajectory of BCI technology is largely unknown. The privacy narrative may very well

---

[180] Coates McCall & Wexler, *supra* note 75, at 9–10, 18.

[181] Shen, *supra* note 77, at 656 ("Current constitutional protections are sufficiently nimble to allow for protection against involuntary government machine-aided neuroimaging mind reading.").

[182] *Id.*

encompass risks that do come to pass. As Shen argues, when we have brain data, we (everyone—the government, industry actors, consumers) should take care to stick to the science. Since the P300 signal does not offer much information about someone's memory, for example, P300-based "lie detectors" should not be allowed to proliferate.[183] But not every concern within the privacy narrative may qualify as a misinformation-fueled panic.

In the next section, I discuss how Bryan Casey and Mark A. Lemley's *You Might Be A Robot* offers a potential method for regulators to address the privacy narrative.

II. LEARNING FROM ROBOTS

In Part I, I presented a bird's-eye overview of BCI technology. I also analyzed a privacy narrative—a discrepancy between the technology's current state and the type of privacy concerns that are routinely voiced in writings and discussions about BCIs. I will now turn to Bryan Casey and Mark A. Lemley's article "You Might Be A Robot" and discuss how their theory about defining "robot" helps shed light on regulating BCIs.

As I explained above BCIs they share many of the same general privacy risks associated with other kinds of IoT and AI devices. Functional criteria, by their nature, are focused on what something can *do* rather than what something *is*—making it possible for one regulation to apply to multiple kinds of devices at once. For the same reason, functional criteria have a better chance of keeping up with the rate of technological change.

Regulating using functional criteria rather than definitions, as Casey and Lemley propose, could help regulators protect against serious privacy concerns without singling out BCIs, which could be wasteful and unnecessarily inhibit innovation. Regulators may develop BCI-specific regulation because the privacy narrative emphasizes the novelty of interacting with the world using your thoughts alone. Elected officials, who lack insulation from political processes and are incentivized to respond to popular constituent concerns, are especially likely to adopt targeted regulation (should BCIs become politically salient enough to garner attention). But any regulator with limited knowledge of available BCI technology could be drawn to the idea that protecting "thought privacy" is a challenge that requires targeted action. BCI-specific regulation, in turn, requires an answer to the question "what is a BCI?" As Casey and Lemley show, definitional questions are both tough to answer and unlikely to result in effective regulation.

[183] *See id.* at 685–86 (describing the scientific shortcomings of the brain fingerprinting approach).

A. Of Robots and Humans (and Cyborgs): Bryan Casey and Mark A. Lemley's Argument

In *You Might Be A Robot*, Bryan Casey and Mark A. Lemley make the case that trying to define robots in order to regulate them is often a losing game.[184] For their own purposes, they employ a subjective definition: a robot is anything that can conceivably be called a robot.[185] Rules and statutes that include definitions, they argue, are very likely to become outdated at an astonishing pace.[186] Even if a regulatory or statutory definition seems to stand the test of time, it may be underinclusive, overinclusive, or both at once.[187] Acknowledging that definitions are sometimes impossible to avoid, they advocate regulators asking whether defining "robot" is necessary as a "threshold question."[188] "[W]henever possible," they suggest, regulators should "establish whether a potential regulated entity is a robot without resorting to explicit, ex ante definitions."[189] Instead of ex ante definitions, regulators should consider functional criteria.[190] In doing so, they suggest that the focus should be on regulating conduct rather than actors or things—"verbs, not nouns."[191]

---

[184] Bryan Casey & Mark A. Lemley, *You Might Be A Robot*, 105 CORNELL L. REV. 287, 293–95 (2020) [hereinafter *You Might Be A Robot*].
[185] *Id.* at 296.
[186] *Id.* at 313.
[187] *Id.* at 315.
[188] *Id.* at 341.
[189] *Id.*
[190] *Id.* at 342:

> Adopting functional criteria, as [Alan] Turing did, makes us less likely to produce definitions that quickly become obsolete. And, unlike formal definitions, the process is also less apt to provide adversaries with a roadmap for gaming or abusing our legal rules. Perhaps even more importantly, clearly establishing functional criteria can also help to reduce confusion by judicial bodies that may subsequently rely on different schools of interpretation to understand a definition. By signaling our legislative intent through functional criteria, legislators and regulators can reduce the likelihood of textualists and purposivists coming out on opposite sides of a definitional debate. This isn't just good legislative hygiene, it's also consistent with the general preference for standards, not rules, when governing fast-changing technology.

[191] *Id.* at 343:

> A focus on conduct, not status, is a good idea for other reasons. It may help us avoid discrimination against certain technologies or business models, and ultimately avoid discrimination against robots. It will allow us to accumulate knowledge and hone our definitions over time by giving us the flexibility to change course as the technology changes. And, ultimately, it may prevent unnecessary regulation by narrowing our legal rules to focus on identified problems rather than creating regulations that apply across the board to robots, whether we need them or not.

Casey and Lemley do not make an argument for or against robot regulation. Instead, they offer a pragmatic take with a somewhat dim (and likely accurate) view of the policymaking process: Regulators will regulate, whether doing so is wise or not, and there are plenty of policymakers who are "untrained, unfamiliar, or unconcerned" with technological matters.[192] For Casey and Lemley, developing truly effective robot regulation is a fantasy. Their goal is damage mitigation. In the absence of truly effective regulation, "less bad" regulation is the next best thing.[193]

Casey and Lemley's top mitigation strategy: Avoid categorical definitions wherever possible. In lieu of such definitions, regulation should include functional criteria for determining whether an entity is or is not subject to a given regulation.[194] They point out that functional criteria is already a *modus operandi* of the common law and that the FTC has made use of the idea with regard to privacy.[195] Because theirs is an article about robots, Casey and Lemley call this strategy "Turing's Razor"—a play on the principle of Occam's razor, which holds that one should use no more assumptions than necessary to explain something.[196] Turing is Alan Turing, a founder of modern computing and a greatly influential figure in the development of artificial intelligence. As Casey and Lemley recount, Turing proposed a functional criterion for deciding whether something qualified as artificial intelligence: "if it behaves in a way indistinguishable from the way intelligences behave," it is intelligent.[197] Of note here is that Turing's criterion targets an action—behaving intelligently—rather than an actor. In Casey and Lemley's words, it targets a verb, not a noun.[198] Regulating verbs rather than nouns will generally work, they argue, because regulation is usually prompted by functionality concerns rather than issues with the regulated entity itself.[199]

A main benefit of Turing's Razor is relative ease of enforcement. Functional criteria, Casey and Lemley argue, can clarify regulations for the judicial bodies tasked with enforcing them by signaling legislative intent.[200] Turing's Razor also offers protection against would-be regulation-dodgers. Functional criteria are harder to avoid than categorical definitions.[201] On the drafting side of things, Turing's Razor may keep regulators from

---

[192] *Id.* at 296.
[193] *Id.* at 336.
[194] *Id.* at 341–42.
[195] *Id.* at 341.
[196] *Id.*
[197] *Id.* at 342.
[198] *Id.* at 342–43.
[199] *Id.*
[200] *Id.* at 342.
[201] *Id.*

unnecessarily targeting particular technologies or potential but unproven risks.[202]

Some regulators are better positioned to regulate verbs than others. When FDA distinguishes between medical devices and wellness devices, the agency is regulating nouns. Although that particular distinction is largely discretionary, FDA's mandate is noun-centric. The agency is responsible for food, drugs (and devices), and cosmetics that fall within the ambit of the definitions laid out in subchapter II of the Federal Food, Drug, and Cosmetics Act.[203] The FTC, in contrast, has a verb-centric mandate. The Federal Trade Commission Act gives the FTC authority to investigate and punish unfair trade "acts or practices."[204] Even industry regulators may find themselves beholden to definitions they cannot easily change. (Industry definitions played a role in the *Frigaliment* case, which I briefly discuss in the next section.)

In short, not every regulatory problem can be solved by thinking about verbs. Casey and Lemley are aware of this and suggest guidelines for those times when you really do need to define "robot." They are also aware of the distinct possibility that regulators will not change the way they regulate; their guidelines work for those situations, too. First, they suggest using categories rather than "a single overarching definition." They note that categories can serve a similar purpose to functional criteria in that they can make it harder for entities to avoid regulation by squeezing into, or out of, a definition.[205] As I mentioned *supra*, virtually no one in the BCI industry wants to deal with expensive, time-consuming FDA premarket approval if they can help it. This creates an incentive to frame BCIs as wellness devices, which are subjected to much less regulatory scrutiny than medical devices.

Second, Casey and Lemley propose regulating rather than legislating whenever possible. Government agencies have more room than legislatures to craft flexible, temporary definitions.[206] Agencies can issue nonbinding guidance documents to test the waters, and rules generally go through a public notice and comment process. Casey and Lemley concede that agencies are vulnerable to capture and that they may struggle to handle the "cross-cutting nature of robots."[207] Indeed, much has been written on the challenges that emerging technologies pose for the administrative state—both regulating

---

[202] *Id.* at 343.
[203] *See* 21 U.S.C. § 321 (defining "food," "drug," and "device").
[204] 15 U.S.C. § 45.
[205] *You Might Be a Robot*, *supra* note 20, at 356.
[206] *Id.* at 358–59.
[207] *Id.* at 335–37.

them and using them.[208] Yet the alternative to agency-industry cooperation is no cooperation, which is not a recipe for effective regulation. Last, Casey and Lemley advocate sunset clauses (*i.e.*, expiration dates) and express opportunities for revision in situations where a statutory definition is unavoidable.[209]

If a statutory definition *is* avoidable, though, what sort of functional criteria should take its place? Casey and Lemley stop short of proposing a definitive set. The idea is not that a single test, like Turing's, is applicable across the board. Instead, they offer six criteria as a starting point: agenda; automaticity; autonomy; agency; ability; and anthropomorphization.[210] "Agenda" is a consideration of the motives behind the development and deployment of robots.[211] "Automaticity" highlights the distinction between robots that can accomplish tasks with no human intervention—fully autonomous robots—versus "autonomish" robots that require some intervention.[212] This distinction becomes important, Casey and Lemley argue, in contexts where human engagement changes the basic regulatory question or automatic actions are considered more (or less) desirable than human actions.[213] Similar to "automaticity," "autonomy" is a consideration of "the extent to which an entity is empowered to make decisions."[214] "Agency" concerns who, or what, should be held responsible for what a robot does.[215] "Ability" follows "agenda," asking not what the intended goal of a robot is but rather how that goal is achieved. Ability is very much *not* a consideration of who or what entity has certain abilities—it concerns the abilities themselves.[216] (This goes directly to Casey and Lemley's central "regulate verbs, not nouns" idea.) Last but not least, "anthromorphization" is a consideration of human reactions to robots.[217]

B. What's in a Name?

---

[208] *See, e.g.*, Ryan Calo & Danielle K. Citron, *The Automated Administrative State: A Crisis of Legitimacy*, 70 EMORY L. J. 797 (2021); David Freeman Engstrom & Daniel E. Ho, *Algorithmic Accountability in the Administrative State*, 37 YALE J. REG. 800 (2020); CARY COGLIANESE, A FRAMEWORK FOR GOVERNMENTAL USE OF MACHINE LEARNING (2020) (report to the Admin. Conf. of the U.S.), https://www.acus.gov/sites/default/files/ documents/ Coglianese%20ACUS%20Final%20Report.pdf [https://perma.cc/L3SG-PJYP].

[209] *You Might Be A Robot*, *supra* note 20, at 360.

[210] *Id.* at 344.

[211] *Id.* at 344–45.

[212] *Id.* at 346.

[213] *Id.* at 347.

[214] *Id.* at 348.

[215] *Id.* at 349.

[216] *Id.* at 350–51.

[217] *Id.* at 353–55.

In tracing the development and wide variety of advances in robotics, Casey and Lemley note that the boundaries between human and machine are growing thinner—not because of robotics alone, but also because of what they term "human augmentation":

> These boundary-blurring technologies include systems such as Elon Musk's "Neuralink," MIT's "Mind-Reading" headsets, and even chip implants that can unlock doors or generate passwords. They also include plant-robot cyborgs that can move themselves toward needed sunlight. The end goal of these "cyborg" or "cybot" applications? To turn human bodies into computers.[218]

I would counter that not every BCI can be comfortably explained as a means of turning the human body into a computer—even those that do seem to fit the term "human augmentation." Some can conceivably be called "human augmentation," others "robots," while still others seem to defy both terms. The IpsiHand BCI that FDA approved as a therapy for stroke patients seems more like a computer helping humans regain lost biological function rather than a computer seeking to replace that biological function. (Maybe that means it is a robot, using Casey and Lemley's subjective definition.) It does change the way the user's brain works, but it does so to help put the user back where they were before the stroke—does that count as human augmentation? Or are such devices, even if they employ AI, a different kind of technology? My quibble with Casey and Lemley's categorization proves their main point. With "boundary-blurring" technologies like robots and BCIs (subjectively defined), resisting their ineffability is futile.

To the extent that BCIs and robots can be distinguished, would-be BCI regulators arguably have additional definitional challenges beyond those that would-be robot regulators face if they seek to develop BCI-specific regulation. As established in the Part I, at least some people are freaked out by the idea of a device that could read their minds. Philosophers and neuro-scholars, to say nothing of generalist regulators, cannot agree on what exactly the mind is.[219] It necessarily follows that there will be ample disagreement over what exactly a mind-reading device is. I argued that consumer BCIs do not read minds in any traditional sense of the term "mind," but someone who holds that all brain activity is mind activity will heartily disagree with me. Is a Muse headband, which tracks certain brain signals and provides a very basic analysis of the user's mood, a mind-reading device? Maybe a brain-reading device? What about BCIs that alert users to impending epileptic seizures?[220] Those devices definitely read the brain. Yet researchers found that some users

---

[218] *Id.* at 306.
[219] Sanders, *supra* note 151.
[220] Drew, *supra* note 28, at S19–S21.

experience significant changes in their identity and understanding of who they are as a "self."[221]

The law is full of definitional challenges. Most people who went through law school will remember *Frigaliment Importing Co. v. B.N.S. International Sales*, otherwise known as the "chicken case."[222] Therein, the esteemed Judge Henry Friendly tried his best to determine what two parties to a contract meant by the word "chicken."[223] For a certain kind of philosopher, no words have set meanings; "chicken" is at once everything and nothing. For the rest of us, many words have one meaning, or a fixed range of meanings. Accordingly, legal challenges to definitions are usually about *who gets to decid*e what a particular rule or statutory provision means rather than *what things actually are* out there in the real world.

Robots and BCIs, however, are utterly nebulous concepts. Ask ten people to describe a chicken, and you are likely to get ten fairly consistent descriptions. Ask ten people to describe a robot—not so much. And if you ask ten people to describe a BCI, you are likely to get at least one response along the lines of "describe a *what*?"

BCIs may or may not be robots. But many contain robots, by at least one definition—they employ AI to make up for fuzzy signals. Although the specifics of the algorithm will surely differ between BCIs, the most common decisional privacy concern—namely the fear of losing one's identity or ability to make one's own choices—implicates the basic predictive feature of machine learning. It follows that "verb-centric" regulation targeting predictive behavior, even if not BCI-specific, is likely to address this common privacy concern. Regulation of the use of predictive algorithms to infer someone's mood, for example, would capture both hyper-curated advertising schemes and a BCI that zaps your brain when you are feeling sad.

---

[221] *Id.* at S21.
[222] Frigaliment Importing Co. v. B.N.S. Intern. Sales Corp., 190 F. Supp. 116 (S.D.N.Y. 1960).
[223] *Id.* at 117:

> The issue is, what is chicken? Plaintiff says 'chicken' means a young chicken, suitable for broiling and frying. Defendant says 'chicken' means any bird of that genus that meets contract specifications on weight and quality, including what it calls 'stewing chicken' and plaintiff pejoratively terms 'fowl'. Dictionaries give both meanings, as well as some others not relevant here. To support its, plaintiff sends a number of volleys over the net; defendant essays to return them and adds a few serves of its own. Assuming that both parties were acting in good faith, the case nicely illustrates Holmes' remark 'that the making of a contract depends not on the agreement of two minds in one intention, but on the agreement of two sets of external signs—not on the parties' having *meant* the same thing but on their having *said* the same thing.

Of course, perfection is too much to hope for in the realm of regulation. There is no guarantee that future BCIs will have enough overlap with other machine learning applications to make that sort of rule feasible. In the meantime, however, overlap is a near certainty. Questionable algorithms are popping up everywhere, leading to increased calls for more scrutiny of AI decision-making.[224] If that scrutiny turned into verb-centric regulation, BCIs would be covered.

The same is true, I argue, for regulation of consumer BCIs and the Internet of Things (IoT). As technology stands now, there is a great deal of overlap between BCIs and other IoT devices. Although the privacy narrative emphasizes the mind as a site deserving special solicitude, verb-centric IoT regulation is likely to prevent many of the informational privacy concerns in the narrative. A rule requiring consumer IoT manufacturers to take reasonable steps to safeguard their products from hackers trying to get users' financial information will work for FitBits, Alexas, and Muses alike. That said, regulators drafting such a rule may need to consider affect in some depth because of the widespread understanding that there is something qualitatively different about taking a PIN from FitBit data versus from BCI data. Leaning into the language of intrusion and surveillance in public education materials about general IoT hacking may be one way of minimizing the normative differences between BCIs and other consumer IoT devices and so blunting the impact of the privacy narrative's emphasis on the mind.

C. Affect: A Functional Criterion for BCIs (and Beyond?)

Casey and Lemley contend that robots are particularly unruly subjects of regulation because they tend to inspire strong emotional responses.[225] As I discuss *infra*, this focus on our emotional connection to robots is one of Casey and Lemley's key insights—and one of the primary reasons their argument is useful for thinking about BCIs.

Treating robots as either human or "dumb machines" for regulatory purposes, Casey and Lemley write, strengthens implicit biases about the motivations, abilities, and limitations of humanlike robots.[226] Humans are likely to assume that a humanlike robot will have the same motivations, abilities, and limitations as a human. Progress in robotics, particularly AI, is often measured in terms of humanness. It may be that some, if not most, robotics experts are keenly aware that "advanced" robots need not bear a resemblance to humans. But as Casey and Lemley note, there is no guarantee

---

[224] Manheim & Kaplan, *supra* note 71.
[225] *You Might Be a Robot*, *supra* note 20, at 313.
[226] *Id.* at 335.

that regulatory experts are also robotics experts.[227] Even if a particular group of regulatory experts *are* experts when it comes to a certain type of robot, that robotics expertise is unlikely to be useful for very long given the rapid development of new technology.[228] Efforts to increase cooperation between agencies, industry and government regulators, and actors with different areas of expertise are underway. Assuming their success, however, is a recipe for ineffective regulation.[229]

Of the six criteria, all except automaticity are self-evidently applicable to BCIs. By their nature, all BCIs include some level of human involvement. They are not fully autonomous, even if they can perform some functions—predicting what word a user is spelling, for example—autonomously. To keep the "A" pattern going, I suggest affect as a replacement for automaticity. Affect flows from the notion of agenda, which Casey and Lemley describe as "the motives held by those deploying robots, which presumably dictate the ends robots will serve."[230] Affect is not motive, but normative power stemming from emotional responses to new things. It does not directly dictate what ends BCIs will serve, but it plays a role in how and the degree to which those ends will be achieved. Affect often goes hand-in-hand with anthropomorphization, too. As Casey and Lemley argue, "[i]f we subconsciously expect a robot to act like a human being, we will be surprised and upset when it doesn't, or when it makes mistakes that seem bizarre to us."[231] One way to understand affect is as an extension of anthropomorphization.

Affect is useful because regulating "verbs, not nouns" opens the possibility of regulation that encompasses BCIs but make little reference, if any, to thoughts or brain signals. Such regulation is desirable in theory for all of the reasons discussed in this Part—but it may be ineffective if it does not anticipate how people relate to BCIs. This anticipation does not require overt references to thoughts or brain signals, of course. That would undermine the benefits of the "verbs, not nouns" approach. The point of affect as a functional criterion is, like anthropomorphization, to remind regulators that people bring their prior experiences and beliefs into their interactions with technology. In the particular context of BCIs, a focus on affect gives regulators dedicated space to engage with the privacy narrative.

A robot example will serve my point here. In mid-2021, the New York City Police Department unveiled "Digidog," a roughly knee-height robotic

---

[227] *Id.*
[228] *Id.* at 339.
[229] *Id.* at 337–39.
[230] *Id.* at 344.
[231] *Id.* at 354.

entity that moves itself on four spindly legs.[232] The agenda: fighting crime. The affect: terror. After a public outcry, the Department returned the "dog" to its creator, Boston Dynamics. Then-Mayor Bill DiBlasio expressed relief at this development, saying that the dog was "creepy, alienating, and sends the wrong message to New Yorkers."[233] To the public, what the dog was actually capable of mattered less than what it looked like it *could* do. Digidog fell victim to the common bias against robots that subvert natural forms. When something has four legs, is about knee height, and walks on its own down a New York City street, most people would expect to see a furry pet—not a lurching, headless thing with blinking LED lights. At the same time, Digidog heightened the concerns of New Yorkers who saw the robot as another means of unwelcome surveillance of their heavily policed neighborhoods.[234] Emotion-charged responses like these are important. They can guide our sense of ethics and help us make connections between things that appear disparate at first approach. The Department saw a tool that could help save money and officers' lives. The message received by people outside the Department was that the police are overfunded and needlessly militarized.[235]

Although adopting functional criteria will not solve the macro-level structural challenges with regulation that I mentioned in Part I, it may help diminish their consequences. In leading regulators to consider emotional responses, affect makes room for conversations about biases—both biases that people may have against certain technologies but also how certain technologies exacerbate existing disparity-creating biases. Even though such biases may not always be captured in empirical data, or reflect some "objective" measure of reality, they should be considered real for regulatory purposes because biases impact how we interact with technology and with each other. In addition, members of marginalized communities whose life experiences have given them anecdotal evidence of systemic bias against them often lack access to the political capital and resources to support that evidence with empirical data. The consequences of systemic bias can thus be left out of regulatory cost-benefit analyses. This focus on the quantifiable can hurt technologies, too, which may be on the receiving end of popular, industry, or governmental biases but offer significant benefits.

The privacy narrative shows that this agenda-affect discrepancy is also present in the BCI context. The Muse headband cannot tell you much

---

[232] Emma Bowman, *'Creepy' Robot Dog Loses Job With New York Police Department*, NPR (Apr. 30, 2021 8:37 PM ET), https://www.npr.org/2021/04/30/992551579/creepy-robot-dog-loses-job-with-new-york-police-department [https://perma.cc/2TS9-8QQ5].
[233] *Id.*
[234] *Id.*
[235] *Id.*

about your thoughts or mood.[236] But the device looks like something that can decipher deep emotional states, at least to those people who are at all familiar with science fiction, and the non-fine print strongly suggests as much. It also looks like something that can be hacked. All this sounds like a false advertising problem, which it is. But there is more to it. People looking for money (or just creating chaos) are more likely to try to hack something that (1) looks like it can be hacked and (2) looks like it collects information that would be valuable to sell or hold for ransom. To put it another way, regulators should be aware that BCIs are especially rich generators of narratives and that at least some people are likely to act on the basis of at least some of those narratives.

Affect in BCI regulation might include a more substantial accounting of what conduct falls within "proper use" and "misuse" of a given product. It could also take the form of details gleaned from outreach to an expanded pool of stakeholders during the drafting process, or a presumption of action in favor of vulnerable or underserved populations when there are multiple courses of action available. Sometimes—perhaps often—regulators will fail to consider how a rule, guidance document, or statutory provision impacts particular communities. With BCIs, regulators (who are likely "able-bodied") are perhaps most at risk of overlooking "disabled" people's views on the devices.

CONCLUSION

This comment has investigated existing BCI technology, regulatory challenges, and the potential application of Bryan Casey and Mark A. Lemley's ideas for regulating robots to BCI regulation. I have suggested that BCIs, a varied group of devices, are both difficult to define and subject to a "privacy narrative." This narrative is a collection of worries and questions surrounding the current abilities and development trajectory of BCIs which appears in the media and in research alike. It complicates regulatory decision-making because BCI technology is still too new for us to know just how far-fetched the idea of a mind-reading device is. Regulating verbs instead of nouns, per Casey and Lemley's argument, means choosing functional criteria over definitions when attempting to regulate. I suggested the addition of "affect" to their list as a means of cabining the influence of the privacy narrative.

---

[236] *See Listen and Explore*, MUSE, https://choosemuse.com/muse-2-guided-bundle/ [https://perma.cc/S66T-AV2F] (last visited Feb. 6, 2022) (advertising the Muse headband as being able to differentiate between three mental states—"calm," "neutral," and "active"—and describing "active" as "wandering attention" state).