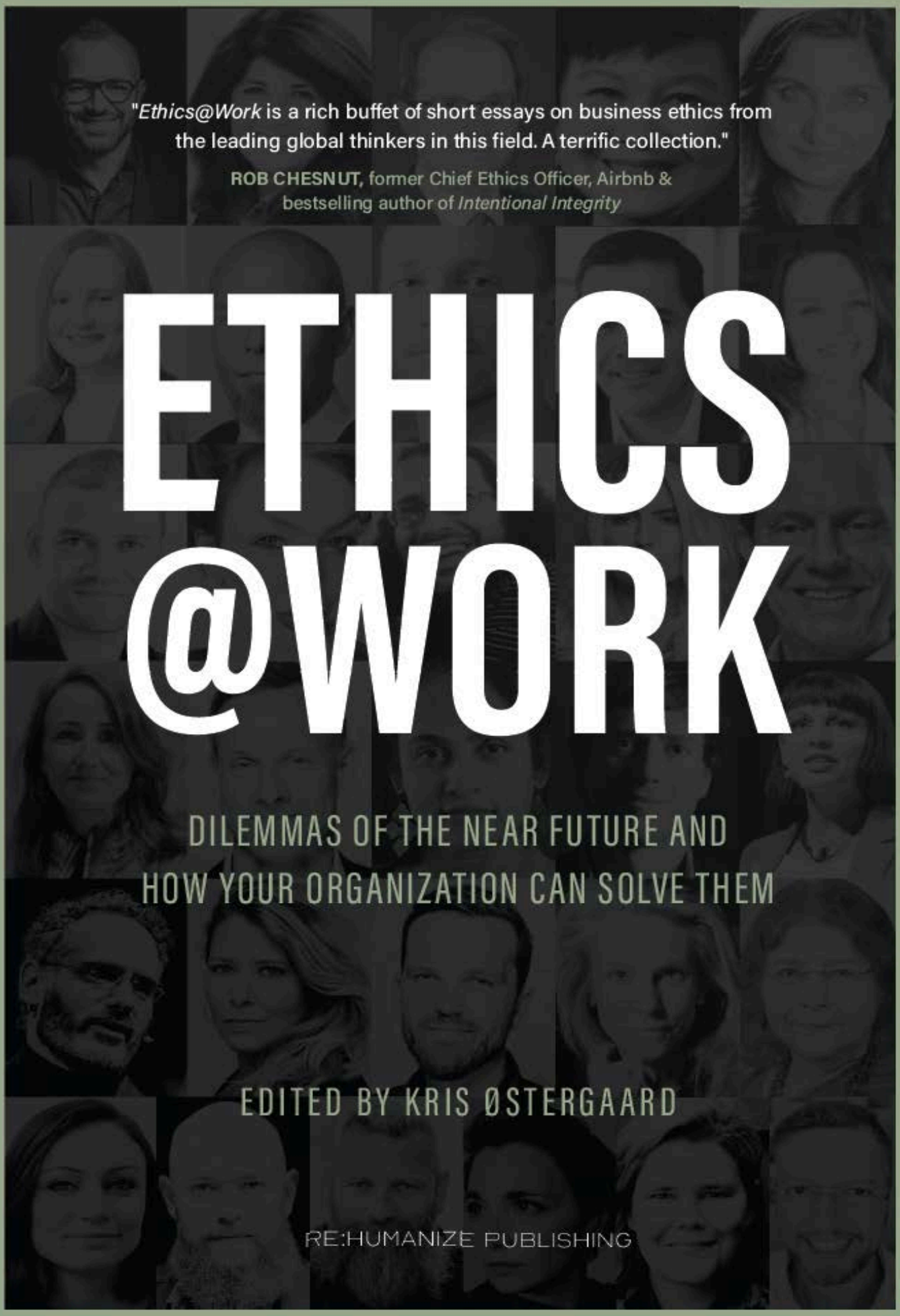
"*Ethics@Work* is a rich buffet of short essays on business ethics from the leading global thinkers in this field. A terrific collection."
ROB CHESNUT, former Chief Ethics Officer, Airbnb & bestselling author of *Intentional Integrity*
ETHICS @WORK
DILEMMAS OF THE NEAR FUTURE AND HOW YOUR ORGANIZATION CAN SOLVE THEM
EDITED BY KRIS ØSTERGAARD
RE:HUMANIZE PUBLISHING

ISBN: 9788797284100 (print)
ISBN: 9788797284117 (e-book)

Date of publishing: February 2022

This book is printed ondemand to reduce supply chain waste, greenhouse emissions, and conserve valuable natural resources. All paper suppliers are expected to be environmentally responsible and not use papers sourced from endangered old growth forests, forests of exceptional conservation value, or the Amazon Basin.

ETHICS @WORK

DILEMMAS OF THE NEAR FUTURE AND HOW YOUR ORGANIZATION CAN SOLVE THEM

EDITED BY KRIS ØSTERGAARD

I THINK, THEREFORE I AM – NEURAL SOVEREIGNTY AND NEURAL RIGHTS IN THE 21ST CENTURY

DIVYA CHANDER

Cogito, ergo sum
René Descartes, Discourse on the Method (1637)

Descartes posited that the thinking mind was axiomatic proof of our existence. Drawing on the logical extension of this axiom, if your mind is what defines you, then do you have the right to your own mind? Do you have the right to "neural sovereignty," potentially the last bastion of Selfhood? Is it more important than even your genome, that other code of life?

Recent advances in neurotechnology have made the science fiction of *Black Mirror* and *The Matrix* science fact. The technologies are glorious, beautiful, and exquisite, and have the potential for creating real human advancement. But the Collingridge dilemma (named for David Collingridge's 1980 book, *The Social Control of Technology*) applies to this technology as much as it does for any of our most forward biotechnological advances, such as gene editing and synthetic biology. Collingridge stated that "when change is easy, the need for it cannot be foreseen; when the need for change is apparent, change has become expensive, difficult and

time-consuming."[46] The challenge lies in being able to predict the potential impact of a new technology to enact policy to stay ahead of it, so that we as an international community and as an evolving ethical species, can anticipate the need for regulation and what limits to apply to it, so that it does not violate basic human rights' norms. Make no mistake—given the enormous power to collect humans' data, the obligations for businesses in today's society are as deep and profound as the obligations of the governments of nation states and international regulatory institutions.

This essay is about exactly this effort—to understand neurotechnology and its cutting edge, and to stay ahead of the effort to self-regulate its misuse, precisely by understanding the myriad ways in which it can be exploited. Companies and businesses that adhere to such principles in advance, should be both recognized and rewarded to encourage the voluntary participation in such initiatives.[47] IBM did exactly this in working towards a crowdsourced, iterative framework for ethical artificial intelligence, which they committed to upholding in their own company and day-to-day practices.[48] Facebook Reality Labs claims to have integrated a series of responsible development principles for their neuro-capable devices,[49] which you will see are not comprehensive given the risks outlined in what is to follow; but paying lip service to this means there is pressure in this domain. Therefore, early adoption of ethical neurobusiness practices can potentially form the basis for helping to craft and accelerate the adoption of ethical neurotechnology principles, as well as trust in your company, its brand, and its uptake.

THE NEW EDGE – HOW TECHNOLOGY HAS ENABLED US TO READ AND WRITE TO THE BRAIN

Everything we talk about next will hinge upon a singular

understanding—that of the neural code, the fundamental code of life that endows us with the ability to exist and navigate the world. In other words, in order to translate stimuli, objects and phenomena, from the outside world, or generated within the organism, what is the alphabet? How do you translate one form to the other? How do you get from the activity of nerve cells to complex percepts? Is the definition of consciousness embedded somewhere in this code, or is it something different altogether?

CAN YOU READ MY MIND?

In 2011, Jack Gallant and his postdoc, Shinji Nishimoto, published a seminal paper in mind-reading.[50] Placing student volunteers into a magnet (an fMRI machine), the scientists presented YouTube movie trailers to the subjects, and measured the brain activity in response to those movies from one of the early visual processing areas in the brain, called the visual cortex. From these neural recordings, they created the equivalent of a data dictionary—linking patterns of brain activity to the statistics and properties of the visual imagery—a fancy way of saying that lines, orientations, edges, movement, luminance, contrast, and color were mapped to a neural code. Using this database of videos and coded responses, the scientists eventually put a new set of students into the fMRI scanners and showed them a different set of YouTube video clips. Using the previously created dictionaries, the researchers were able to grossly decode the images that the subjects were seeing, even though they were "blinded" or unaware of the video clips being shown.[51] A few years later, Japanese researchers in Kyoto accomplished a similar feat, this time by identifying the visual content of subjects' dreams.[52] In fairness, the algorithms did not actually reconstruct subjects' dreams as the Berkeley group had been able

to do for subjects viewing natural images. But dream content is still a step forward. Though in terms of privacy:

In the years since, the Gallant Lab has created a number of interactive viewers[53] that have explored how the brain represents and encodes semantic data, including its response to storytelling, one of the most natural things we do as social animals.

There are multiple modalities of non-invasive brain reading. Gallant's work is based on the changes in blood flow in the brain measured in a magnet, functional magnetic resonance imaging (fMRI). Other forms of non-invasive brain mapping include the electroencephalogram (EEG), the magnetoencephalogram (MEG), and near-infrared spectroscopy (NIRS). While fMRI and MEG are currently bulky and obvious, the EEG is being progressively made more accessible and portable (see companies like Emotiv, Neuroelectrics, Neurosky, and open-source initiatives like OpenBCI). Openwater (Mary-Lou Jepsen, Founder-CEO) and Kernel (Bryan Johnson, Founder-CEO) are attempting to make smaller and more powerful non-invasive imaging in the infrared (NIRS) and using MEG to see into the brain and map its functionality. Their devices are initially intended for a medical and research community, but they plan to make them ultimately available to consumers.

The main uses for brain decoding have been their applications for understanding the neural correlates of behavior and perception, diagnosing and performing biomarker discovery for neurological disease (e.g., Alzheimer's, schizophrenia, addiction), and creating closed-loop systems for enabling people with functional limitations to interact with the outside world. Acoustic decoding enabled one of the earliest brain-computer interfaces to emerge—the cochlear implant. By understanding how the brain decodes sound waves of different frequencies, a decoder plus electrical stimulator device

can bypass a damaged or non-functional hearing apparatus in the periphery, and convert sound waves to electrical signals that stimulate the cochlear nerve, thus providing a rough way of bringing sound into the brain for those who cannot hear. Similarly, for people who have limitations in sight, understanding the neural code for vision, as early as nerve cells ("neurons") in the retina at the back of the eye is an important step (the retina is a piece of the brain sticking out beyond the skull that binds visual information, or photons of different wavelengths, from the outside world). Understanding how neurons encode, filter, and compute information forms the basis for creating retinal and visual prosthetics that can bypass damaged or incompletely formed areas of the eye, transmitting light and form to places in the brain that can make sense of it. As we speak, bionic eyes and other visual prosthetics are taking off.[54] [55] [56] In addition to supplementing vision for those with retinal damage like macular degeneration, a group in Hong Kong recently published a study in which they created a curved visual prosthetic, with nanowires functioning much the same way as optic nerve fibers do (the highway on which information bits travel from the eye to the brain).[57] The prosthetic's resolution is currently significantly inferior to the human eye, but the researchers anticipate this will improve with time. Their goal—ultimately, to make bionic eyes for robots that can see better than human eyes, yet make the robots themselves appear to be more human. Recently, high-functioning robots are turning out to be quite creepy (for reference, see the Headless Boston Dynamics Dog).[58] [59]

Despite early work in sensory systems, the majority of the exceptionally highly visible/profile advances have taken place in the space of movement. For brain-machine interfaces to work, brain mapping has to be of sufficient accuracy to understand how the brain is perceiving (sensory), planning, or creating intention to do things (motor). Because planning motor activities, like the

trajectory of movement of one's limbs (How would I throw a baseball with my right hand? How would I pick up the orange with my left? How do I move my feet to tango?) is highly mathematical, this code is easier to understand, and to translate into electrical signals that can drive computer monitors, mice, and other actuators outside the brain like robotic arms[60] and exoskeletons.[16]

Another general principle—non-invasive brain readers have less fidelity and accuracy than invasive ones. That is why the potential for closed-loop systems built with invasive interfaces (i.e., electrodes touching the brain) is higher than for non-invasive ones. The Braingate2 Consortium,[61] an academic group of researchers mostly working with tetraplegics (patients paralyzed from the neck down) has shown amazing promise. An array of 96 metal electrodes can be implanted into the motor cortex of these patients, which receives signals for planning motion from upstream parts of the brain. Over time and multiple trials, the chip learns what the intended motion is (much like the algorithms in the Gallant Lab learned to make sense of what subjects were seeing). The decoder can then bypass the damaged motor tracts in the brain, spinal cord, or muscles and direct an actuator outside the subject to perform the intended movement (like a robotic arm bringing a water bottle to a subject's mouth, or using a keyboard to type onto a screen). New advances have been made by the consortium in terms of wireless interfaces to the skull,[62] and the ability to decode imagined handwriting, and turn that into typed words.[63] These connections to computers outside the brain can even enable one to surf the internet with one's mind.[64] Elon Musk's Neuralink has gained a lot of social media exposure for taking this technology to the next level, by reducing the diameter of the electrodes, increasing the packing density, decreasing the heat generated and decreasing the power requirements of these invasive brain-machine interfaces.[65] Despite talk of wanting to create humans that can outcompete AI,

Neuralink's first target, like Braingate's, is also people with paralysis to restore movement to them. The value that Neuralink brings to this endeavor is that Musk can fund rapid technological breakthroughs at a rate that it is hard for government-funded projects and academic centers to match.

YOUR BRAIN WAVES CAN UNIQUELY IDENTIFY YOU

Reading brainwaves provides some additional surprises. Non-invasive EEG and fMRI patterns can identify certain kinds of neurological diseases, or even tendencies. In other words, they can serve as a biomarker for a disease state. Several studies have shown that EEG can pick up alcohol addiction tendencies or schizophrenia by looking at brainwave patterns. Could future employers or health and life insurance companies make using a brain-reading device mandatory, just as some do for urine drug screenings, height, weight, and blood draws? Could this be made a condition of employment? To determine if you are insurable? Even more interesting, Dr. Sarah Laszlo's lab found that using non-invasive EEG caps enabled her to read the summed electrical potentials on the surface of the skull evoked by looking at images—and that the shapes of these potentials were so unique to the individual, they could identify them with 100% accuracy—a *brainprint*.[66] This use of brainprinting could be mandated by organizations, employers, or even financial institutions in the near future, to authenticate an individual. What if large tech companies started to require this to unlock your smartphone, or activate Alexa? Would they then own your brainprint? Could that be combined with a number of other biometrics to create a deep fake of you?

YOUR BRAIN WAVES AND YOUR BODY CAN BE HACKED, LIKE A SMARTPHONE

In 2017, an interesting study was published in Financial Cryptography by Neupane, Rahman, and Saxena, at the University of Alabama.[67] The researchers were looking at commercially available EEG headsets that could be used for mind control during gaming. They found that if the subject paused a video game and logged into a bank account while wearing an EEG headset, they were at risk of having that password stolen. They tested this in 12 subjects, by asking them to type a series of randomly generated PINs and passwords into a text box as if they were logging into an online account while wearing the EEG headset. The act of typing in a password into a screen-based login involves visual processing, and motor movements. If a malicious program had gained access to the device's software and was training itself on the subject's typing and brainwaves (much as algorithms were trained during Dr. Gallant's experiments in visual mind reading), that program might be able to "read" the password. It turns out that just 200 characters were enough for the algorithm to train on a user's unique brain wave response to visualizing and typing in keystrokes corresponding to those PINs. The algorithms decreased the odds of a hacker's guessing of a four-digit PIN from 1 in 10,000 to 1 in 20; the odds of guessing a 6-letter password decreased from about 1 in 500,000 to approximately 1 in 500. And the only solution to protect ones' brainwaves from being hacked was to introduce noise. One scenario that Dr. Saxena painted was "in a real-world attack, a hacker could facilitate the training step required for the malicious program to be most accurate, by requesting that the user enter a predefined set of numbers in order to restart the game after pausing it to take a break, similar to the way CAPTCHA is used to verify users when logging onto websites."[68]

How many enthusiastic gamers would recognize this risk while playing video or virtual reality games? Many of them are already actively "contributing" their brainwave data to the refinement of algorithms that make mind control of avatars, controllers, and video actuators more precise. Oculus is now requiring that its users log in with their Facebook accounts. Currently, data breaches and ransomware attacks are prevalent. A hacked Facebook account could be used to gain illegal access to one's headset, and therefore, an individual's biometrics and brainwaves. That is in addition to the risk of Facebook owning all that neural data.

Medtronic was the subject of a "white hacker" break into some of their best-known, life-saving medical devices.[69] Both their pacemakers, and mini-insulin pumps, when connected to the outside world for software updates, device programming, and interrogation, could be controlled by outside (good) hackers to either deliver aberrant shocks or electrical signals to the heart, or abnormal doses of insulin to the bloodstream. Both shocking the heart or over/underdosing someone with insulin could be fatal. This prompted a 2019 FDA recall of the remote controllers for Medtronic's mini-insulin pumps,[70] and a reworking of their cybersecurity. Other companies creating implantables, like Abbott and Boston Scientific, are now similarly invested in cybersecurity.[71]

WRITING TO THE BRAIN'S HARD DISK

In light of this, could writing to the brain be possible? In fact, yes. Medtronic, Boston Scientific, and Abbott make invasive deep-brain stimulating (DBS) electrodes that deliver electrical stimuli to the brain, and rewire brain circuits in order to treat the symptoms of diseases like Parkinson's, epilepsy, and obsessive-compulsive disorder. As an example:

"Abbott DBS operates with Apple iOS software and controllers for a possibly more familiar interface and easier programming experience. Abbott's new technology, the first of its kind in the United States, also allows people with these devices to communicate with their clinician and receive DBS adjustments remotely, from their home or other location with Wi-Fi or cellular access." [*Emphasis mine.*][72]

The newest DBS device approved by the FDA in 2020, Medtronic's Percept,[73] can both sense and record an individual's unique brain signals, to enable symptom correlation with local electrical field potentials, precisely because these electrodes touch brain tissue. While this might enable more precise DBS adjustments for better control of symptoms and side effects, without the appropriate cyber controls, remote sensing, writing, and machine learning could be used to take invasive control of brain circuits. While they could not write just anything to the brain, they certainly could affect the circuits and resulting behaviors that formed the pathway in which the electrodes were embedded.

For the subjects of the invasive electrode implants, writing to those circuits *remotely* might also be possible in the future, as the electrodes are usually bidirectional (capable of reading neurons as well as stimulating them). That would mean that a population of humans for whom these implants were necessary to overcome disability would be vulnerable, in the same way subjects with pacemaker or insulin pump implants are. More alarming is the possibility of this extending to a larger swath of the population. The hype around companies like Neuralink is partly fueled by people like Elon Musk, implying that individuals might choose to get these minimally invasive implants in the future to enhance themselves, rather than treat dysfunction. If that were to happen, the population of vulnerables open to neural hacking becomes much greater—in cyber terms, the threat radius markedly enlarges to augmented humans.

Others have wondered if non-invasive control is possible. Most of our non-invasive brain rewiring technologies like transcranial electrical and magnetic stimulation, or focused ultrasound, would be near impossible to do without knowledge and consent since they involve an apparatus to be applied to the outside of the skull that is not subtle. (Notably, this does not eliminate the possibility of coercion, i.e., enforced compliance for the sake of employment, money, etc.). But some of the cyberattacks on U.S. embassy officials in places like Cuba and China[74] [75] seemed to involve potential microwave, or pulsed RF warfare directed at the brain, causing intolerable pain, headaches, disrupted sleep, mood, and unwanted sensory experiences. To date, there are no declarations on banning the use of this type of warfare using non-invasive energy, though some are suggesting that international guidelines on "biological" warfare be applied to regulating these use cases.

A FEW OTHER SCI-FI POSSIBILITIES – TELEPATHY, THE METAVERSE, AND IMPLANTED MEMORIES

Some other extraordinary examples of brain read-write technology have occurred in recent years. Non-invasive brain reading (EEG) was used to transmit bits of information through the internet to a non-invasive brain-stimulating device (TMS) in 2 or 3-brain networked situations.[76] In one case, the thought of a foot or hand was delivered seemingly "telepathically" by connecting a sender and receiver's brain through the internet.[77] A similar feat was achieved with 3 brains engaged in a social network ("Brainet") that could solve problems and play games together.[78] The most likely scenario is neurogaming enthusiasts who are already trying to connect to the virtual world by connecting their brainwaves to the metaverse. The metaverse is considered a collective virtual shared space,

created by the convergence of virtually enhanced physical reality and a physically persistent virtual space, including the sum of all virtual, augmented worlds and the internet. This may form the backbone for a parallel reality for many, just as the internet is for us today. If a user's equipment is hacked, information sent could be either read, or manipulated by brain-writing techniques, for nefarious purposes.

Researchers in Tonegawa's Lab at MIT demonstrated in 2013 that it was possible to record memories from mice that had experienced them in one setting, and use those neural recordings to create false associations that had never been experienced before.[79] They were essentially moving memories within an organic brain, creating new contexts. This is not too different than what the character, Neo, experienced in the film *The Matrix*, when his brain was uploaded with patterns for jiu-jitsu. Later, this memory implanting technology was extended to using optogenetics (light-activated, genetically addressed, ion channels in the brain) to write new engrams to brain circuits that had never experienced a memory.[80] This is quite extraordinary—if memories can be created de novo, just by knowing the neural code, terrible memories and associations that contribute to mental suffering, like PTSD, can be similarly erased. But with coerced access to neural circuits, in the future, an individual wanting to be malevolent could hack those circuits, and rewrite them with specific memories or associations.

NEUROGAMING

We've alluded to gaming in several places. Gaming presents an interesting possibility on both the read-write levels, and interactions with the emerging metaverse. We highlighted how engagement and identity might be read. Based on biomarker discovery using fewer

and fewer EEG leads, your brainwaves might give away your addiction potential or predisposition to developing anxiety or depression. Manipulating you to log into sensitive accounts and enter PINs could result in password theft. But the really frightening part of neurogaming is the potential for digitally twinning you.

We've already seen that machine learning coupled with ever more powerful computing chips is enabling intelligent algorithms, with minimal data on your facial expressions or voice, to create a realistic simulacrum of you, a so-called "deep fake." Facebook's CTRL Labs wristbands can use EMG-based (muscle) activity to "read" your limbs' low-energy gestures to do things like control objects in the real world, or in VR, mapping how you move.[81] Biometric data (brain waves, eye-tracking, heart rate, sweating, pupillary dilation, gestures, voice) collected from an individual while responding to natural world simulations in order to improve an avatar's function in the virtual world could enable the ultimate deep fake, a complete digital avatar of you. Some companies like Singularity Studio are already working on 3D avatars, built on DNA Block,[82] to create digital twins that can do your job or train others to, at an enterprise level. In these scenarios, identity theft would be difficult to prove. A near-facsimile of you could fool family members into paying ransom on your behalf, could open bank accounts, impersonate a company CFO to commit wire fraud,[83] or commit federal crimes in your name.

NEUROMARKETING, NEUROCAPITALISM, AND NEUROSURVEILLANCE

The ultimate, seemingly benign use of neural data is to further the cause of capitalism. Neuromarketing has become a field unto itself. It is part of the curricula of business schools, and scores of self-made consultants as well as startups exist in the space to provide

neural data to companies looking to sell products and perform customer research. Using increasingly consumerized neurowearable devices, one can use brain waves to measure engagement with a product, or even an idea. Other biometric data collection can also give away the secrets of the nervous system—an excited subject might have dilated pupils, a faster heart rate, or spend more time scanning an object they find interesting with their eyes. They may sweat more, and have a change in their galvanic skin response. They may exhale more CO2.[84] All these little signals can be a surrogate for interest, sometimes that the subject isn't even consciously aware of. This might enable mass marketing studies, or even rapid brainstorming or prototyping, saving time and money to a company engaged in customer research. However, these signals can be exploited, and also warehoused for future use. For instance, even though you did not provide explicit consent, many stores will use cameras to passively read your interest and engagement with their products and displays. Alexa can listen to changes in your voice, and coupled with AI, detect a change in your health, or engagement with a product, song, or device. As of this writing (June, 2021), a company called Alfi Inc. announced they have forged a deal with Uber and Lyft to provide 10,000 screens to drivers that show ads and other content, while using cameras and facial expression algorithms to determine passenger engagement. These are to be rolled out in Miami, Florida, to start, but will expand to other cities. Consumer choice, consent, or opt-in is not part of the conversation at this moment (for instance, could you specifically request a rideshare car that *does not* have this technology for scanning your face and reactions? Can the screen be turned off at the rider's request? Since drivers make money using them, would that affect the rating they give to riders?). On June 29, 2021, a Silicon Valley startup called Worldcoin, which counts Sam Altman, the Co-Founder of Y

Combinator, as part of its founding team (backed by Andreessen Horowitz, Reid Hoffman, and Day One Ventures) claimed they will be able to provide a Universal Basic Income and democratize access to cryptocurrency by having one exchange it in response to a scan of their iris (part of the eye).[85] This has a number of privacy groups completely concerned[86] —if someone hacks your credit card, or digital account, you can get a new one. You cannot easily get a new eyeball.

In certain countries, these types of data gathering have become more and more commonplace, and the use of that data less regulated, and more obscure to the person from whom the data is being collected.[87] Further, even though certain types of data are protected (e.g., your financial details while you are shopping online at a store), other biometric data are not (e.g., facial recognition within their physical stores). Even worse, if there are regulations in place, these rules regarding your sovereignty do not follow you around, they track and morph with the jurisdiction. Your ultimate self in this scenario is not really sovereign. It depends on how you and your data are viewed across arbitrary lines drawn across the globe. One has to ask how meaningful those geographical lines are given that the data we are speaking of exists in a purely digital form. Soon, humans may as well.

This foretells of an increasing geopolitical versus individual tension regarding neural rights.

DO WE NEED NEW RIGHTS?

If you believe that these things are true:

- Each human being has the right to mental privacy;
- Each human being has the right to own and control their brain's data and identifying features;

- Each human being has the right to freedom from mental manipulation (their free will);
- A person's brain, mind, psyche, and memories are part of one's very Selfhood, and neural rights can be considered human rights...

... then we should be arguing for *a new code of ethics surrounding neural data* and define human rights' principles that will safeguard them. Those principles should be drafted and reinforced by governments of the international community, and followed by independent adjudicators. They should also be willingly undertaken by companies in the private sector, especially as there really are no geographic boundaries any longer within which companies operate.

WHAT SHOULD GOVERNMENTS DO?

There are several ways to protect our neural rights. These might follow one of several models, well described by Rafael Yuste, one of the founders of the NeuroRights Initiative at Columbia University.[88]

Your data could be considered as your:

1. Digital exhaust – these are the breadcrumbs you leave behind on websites and social media platforms you engage with. The most rigorous digital personal rights are the EU's GDPR. Despite the right to privacy being considered a human right under EU law, it doesn't come close to protecting what might be considered the most consequential data you produce.
2. Medical data – in the U.S., medical data is specifically protected by the Health Insurance Portability and Accountability Act (HIPAA), whereas in the EU, it is protected to varying degrees by the local implementation of GDPR. Still, medical

data has fairly strong legal protections around its ownership and sharing.

3. Genetic data – within the EU, genetic data privacy also comes under GDPR, but as with medical data, specific rules are drafted and deployed by country. A law called the Genetic Information Nondiscrimination Act (GINA) in the U.S. prohibits employment and health insurance discrimination on the basis of your genome sequence. But it does not necessarily impact its collection or security, merely its use.

The alternate and most comprehensive viewpoint is that your neural data, given it may be considered to be commensurate with your Selfhood, should enjoy the highest levels of protection. These rights should be considered a territory of Absolute Sovereignty, and should be protected as human rights. Your neural data should also never be used against you—either to discriminate, or to hold you accountable for thoughts you have, even if you have committed no actions (otherwise, we could embark on a Minority Report-like future). And neural writing technologies for forced coercion should not be legal.

Yuste and other scientists and ethicists around the world consider that neural data is commensurate with Selfhood, and should be afforded the highest protections. This is a position I agree with, especially as the unimagined consequences and potential misuse of this data will only increase with time. Chile has written a Neuroprotection Bill of Law into its new Constitution. OECD nations have outlined a privacy framework that touches on ideas such as security, collection and purpose limitations, and consent. For the reasons discussed above, these probably do not go far enough. Even the United Nations High Commission in 2018 defined a Right to Privacy in the Digital Age. From General Comment 16:

"Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant."

Others have advocated that a section on neurorights be added to the Universal Declaration of Human Rights. And two existing U.N. treaties, the Biological Weapons Convention (BWC) and Chemical Weapons Convention (CWC), could be updated to limit abuses of brain technologies. These documents did not anticipate future technologies, and weren't written in such a way as to cover all emerging weapons, or misuse of neurotechnology. Because neuroweapons do affect the brain as a biological system, the BWC could be modified to include prohibitions against the use of weapons to target the nervous system.

WHAT SHOULD BUSINESSES DO?

Sell privacy, not people.

The first point of merit is that if your only business model for making money and scaling is predicated upon taking people's data without consent or obfuscating its collection, selling it to the highest bidder, or using this data without the data producers having knowledge about how it is to be used, perhaps your company needs a new business model. In fact, consumers are becoming increasingly concerned about their privacy, data, and how that data is used, and one can make money protecting and securing data, rather than exploiting it. Pavel Durov, CEO of Telegram, noted that in January 2021, when Facebook changed its privacy policies around the supposedly secure WhatsApp platform, the industry noted the largest mass digital migration in history. In 72

hours, Telegram gained 25 million new users, including heads of state. Durov feels that people no longer want to exchange their privacy for free service and "no longer want to be held hostage by tech monopolies that seem to think they can get away with anything as long as their apps have a critical mass of users."[89] Some companies have already built a business model around collecting and selling individuals' data. There are ways to potentially migrate this to privacy-centered models of data protection, by charging a premium for privacy as an upgrade, and using this as an interim business model till such a migration is complete. This also increases transparency for the consumer regarding how their data is used. We don't want this freemium model to be the only ethical business model surrounding data—the risk is that we will create a future in which only the wealthy can purchase their privacy and have security, and that is not the distributed, abundant future we want.

Do not simply exploit addiction centers in people's brains to sell a product.

Marketing can light up reward circuits in the brain.[90] [91] Although advertising is a necessary part of the growth of a company, if utilizing knowledge about a person's attention and engagement is solely to engage in neuro-manipulation (as an example, see social media algorithms),[92] by driving the addiction centers in people's brains, then perhaps the company would be better served by a different product or business model.

Security and privacy should never be an afterthought.

In any system in which there is a flow of data, the security and privacy should be included from the ground up. That includes the cryptography used in the application layer (the part that faces the consumer on their edge device), the security of the architecture of

the data fabric and network used to store and exchange data, as well as the permissions used to authenticate users that come onto the network. This should hold for both data producers and requestors.

Do not collect or store user data if you do not have to.
This should be self-explanatory. Given the proliferation of cheap computing and chips that outstrip the pace of Moore's Law,[93] AI at the edge (on local devices facing the consumer or user), not just in the cloud, is being enabled. Do your intelligence and sense-making at the edge when possible, so you decrease the risk of a consumer's data being exploited or hacked.

Incentivize people not to give up their neural data and be transparent when they are.
Many consumers are unaware of the consequences of giving up their data. For example, gamers using neurowearables in the AR/VR/XR (mixed reality) spaces believe that sharing these datas might aid in developing neural signal-based control devices or more realistic avatars, creating more authentic gaming experiences. But these things could be accomplished at the edge, without giving up control over this sensitive biometric data. Other consumers may participate in neuromarketing schemes. If there is good reason to share their neural data (e.g., with pharma companies for biomarker research), then:

1. Build in guardrails for transparency (what am I giving up, how will it be used?);
2. Make a user's data rights easy to understand, and not embedded in 5-point font legalese;
3. Use systems that enable the consumer to transact with their data (e.g., give them the means to sell their data to requestors they think may use their data for a legitimate cause), and
4. Provide a system for expiring authorization, or the means for actively revoking authorization to use that data.

There is another real concern for consumers that are incentivized to sell their data. Are we creating a two-tiered market system in which those who have less power or means are incentivized to sell their data while those who can afford privacy do not? If you liken your biometric data to one of your organs, you can see the parallel. There are people without means who feel pressured to sell a kidney. What about their brain's data? We do not want to find ourselves in a world in which neural privacy and security are only the right of the wealthy.

Erase people's data if they revoke consent.
It is possible that a user may consent to data collection or data use and then change their minds. A mechanism for deleting their neural data, along with their memories and any downstream constructs such as a simulacrum or data-based avatar, should be built into the system and easy to activate.

Define your ethics early.
Create ethical frameworks as soon as you create your company. Draw your lines in the sand. Every time you create a new product or service, use that framework as a barometer. Does your product and updated business model comport with the guidelines you originally set? Or is there the potential for misuse, which would violate your ethics? If so, don't do it. Or find ways to build in the protections.

Constantly assess whether your incentives align with your ethical principles.
As your company scales, is your growth strategy consistent with your ethos? Is it consistent with the principles of doing no harm? Of not violating a person's Selfhood and right to mental privacy? Find ways to reward others in the system for doing the right thing,

and form alliances with other companies that maintain this ethos. Create an ecosystem that is aligned with this vision.

Constantly pressure-test your system.
Get periodic feedback from neutral third parties, cybersecurity professionals, and consumer groups to see if you are meeting your security and neural protection goals.

CONCLUSION

"Nothing was your own except the few cubic centimeters inside your skull."
– George Orwell, 1984 (1949)

In 1949, even in the dystopic world of George Orwell, he conceived of a world in which your brain and your thoughts were the last bastion of personal privacy. But the idea that your thoughts are yours may be a passe phenomenon in today's technological landscape.

We live in a world full of enormous possibility thanks to advances in technologies to read and write to the brain. We have also created systems in which the brain can connect to computers, machines, robots, and other actuators outside itself, giving function back to those who have lost it. There is also an entire augmentation movement in which brain-to-machine interfaces are being used to confer new senses and capabilities to humans—superpowers, if you will, forcing the brain to evolve under this new pressure. It is therefore incumbent upon us to anticipate the other edge of the sword of technology, its potential for dual use. Unlike many other kinds of tech, the brain and its neural code go to the very fabric of who we are. It is integrally associated with our Selfhood

and autonomy. This makes it deeply important and timely to consider the ethical ramifications of this technology now. While we are already having conversations around technology companies tracking our digital breadcrumbs and where our attention goes, data generated by the nervous system and read by passive systems, including neurowearable devices and cameras, might easily capture unconscious thoughts and feelings. This makes this data especially vulnerable to violations of principles of consent and privacy. Already, algorithms are being deployed to influence our thoughts, behavior and attention. Neurotechnology is more insidious and more powerfully invasive, potentially altering free will. In the face of this, principles of transparency, autonomy, privacy, consent, self-determinism, and free will become extremely important. The right, also, to mental augmentation and cognitive enhancement also becomes a concern—if only the wealthy and powerful have access to it, it will further accelerate a process of human-directed evolution that we are already seeing, one that exacerbates the fracture lines between the haves and have-nots. Privacy and freedom from manipulation might also become the purview of the rich. I propose some methods by which governments and businesses might consider the implications of this technology so they can anticipate them and act within strong ethical frameworks. We are only as strong as the most vulnerable amongst us.

DIVYA CHANDER

Divya is an anesthesiologist and neuroscientist who also works at the intersection of human health, data, technology, and data security. She is a practicing physician, Singularity University Chair of Neuroscience (and Faculty of Medicine), and Senior Nonresident Fellow at the Atlantic Council GeoTech Center. She leads two companies she cofounded during the pandemic—Lucidify, a remote brain monitoring platform for the detection of

delirium, and Plexxus, a company building the platform to support telehealth and the world's connected global immune system.

Divya also served on a NASA task force for COVID-19 and has co-chaired and directed the post-pandemic global health initiative for OneShared.World. Her research interests center around mapping consciousness, how consciousness will be altered by human augmentation, and how mapping consciousness in humans may enable us to recognize it in nonhuman, intelligent beings (both on and off-planet, e.g., through initiatives like SETI, where she joins the newly formed SETI Complexity Group). She also works in space life sciences and medicine.

"*Ethics@Work* raises important questions regarding how we think about the future of work, humanity, and our value systems and provides excellent tools for smart decision making. Kris has a storied career in thinking about these challenging dilemmas, and in this anthology, he helps others identify and disentangle some of the most complex ones facing organizations. A must-read!"

SHIZA SHAHID, Co-Founder, Our Place and Malala Fund

"Stellar thinkers take us on a breakneck moral journey from exponential economics through corporate activism to sentient machines. A powerful, provocative guide to our shared ethical futures."

CENNYDD BOWLES, bestselling author of *Future Ethics*

"So, you think you're ethical in your work? What if I told you that digital and a global pandemic moved the goal posts and continue to do so without our knowing or acknowledgement. *Ethics@Work* helps us re-center ethics for the next normal."

BRIAN SOLIS, 8x best-selling author, incl. *LifeSCALE: How to Live a Creative, Productive, and Happy Life*

"As an entirely new economy driven by artificial and autonomous intelligence emerges, what role will our traditional senses of work, ethics—and fair play—play? To what extent will these values be usurped by processes optimized for expedience and profit? How will we navigate their myriad unintended consequences? Indeed, what lies ahead in our very understanding of the term "human resources?" These are the questions taken head-on in *Ethics@Work*—a fascinating compendium of thought leaders whose insights show the clear way forward for us all."

JOHN SCHROETER, Executive Director of Abundant World Institute and editor of *After Shock*

"*Ethics@Work* is a rich buffet of short essays on business ethics from the leading global thinkers in this field. In our increasingly crowded and connected world, the issue of how we can be good to each other has never been more urgent, and this book takes it on from all angles. A terrific collection."

ROB CHESNUT, former Chief Ethics Officer of Airbnb, bestselling author of *Intentional Integrity*

ISBN 978-87-972841-0-0