NEUROTECHNOLOGY AND MENTAL PRIVACY: LEGAL CHALLENGES OF BRAIN-COMPUTER INTERFACES IN THE DIGITAL AGE

Anshul Kumar Manik, University of Allahabad

ABSTRACT

The rapid development and commercialization of Brain-Computer Interfaces (BCIs) have converted neurotechnology from a niche medical research innovation into a consumer product, spanning industries such as healthcare, workplace monitoring, gambling, education, and smart devices. As the technological systems grow more capable of direct neural intervention, they will begin generating neural data that will not only sum up an individual's conscious thoughts but all of his or her subconscious mental processes, emotional reactions, intentions, and behavioral predispositions. This new reality will give rise to significant new legal and ethical questions concerning human dignity and privacy rights. This paper postulates that while a host of personal data protections, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), protect some categories of personal neural data, the existing data protection principles will be inadequate to protect the ever-expanding categories of inferred neural information derived from BCIs. It compares existing privacy laws, constitutional data privacy protections, and emerging BCI regulatory regimes, to highlight the current lack of a legal framework for protecting the cyber-physical inferred neural information obtained from biometric psychographic profiling. It argues that BCI and neuro artificial intelligence (AI) convergence will emerge with psychiatric, governmental, and corporate cyber-neuro-surveillance, neuro-effects, "brain jacking," and behavioral manipulation, warranting a three-neuro rights system of cognitive liberty, mental privacy, and mental integrity to safeguard human dignity by establishing, supporting, and enhancing a new legal paradigm protecting this galvanic neural data. It concludes that ANI is better prepared to anticipate and circumvent this new wave of existential neuroweapons if this new legal paradigm can be enshrined as a third pillar of AI physics alongside Newtonian gravity and quantum physics.

Keywords: Brain-Computer Interfaces (BCIs), neurotechnology, neuro data, mental privacy, neuro rights, cognitive liberty, mental integrity, artificial

intelligence (AI), data protection law, privacy law, cybersecurity, brain jacking, neuro surveillance, neuromarketing, and human rights, highlighting the emerging legal and ethical challenges associated with protecting cognitive autonomy and neural information in the digital age.

Introduction

The human mind has long been considered the last barrier of individual privacy[1]. Governments, organizations, and individuals have always had the tools to watch actions, listen to conversations, and direct behavior[2]. Thoughts, however, could not be reached: the natural division of inner mind and outer observation has been a pillar of human dignity and freedom of thought[3]. For example, legal doctrines throughout the world have, for the most part, assumed that a person 's mental states are inherently protected because they cannot be observed[4]. As a result, explicit legal protection of the mental privacy has previously not been deemed necessary.

The idea that raw brain data can never be intelligibly transmitted or understood by anything other than our own consciousness has also been challenged by the development of future technologies such as Brain-Computer Interfaces (BCIs)[5]. BCIs can be thought of as systems that transfer information between the brain and an external computer system, converting brain signals for apparent later use[6]. Although their technological origins lie in fields of medicine designed to support the disabled or neurologically compromised (encephalography, amniocentesis), the sciences are flourishing in consumer products and service markets. With a rapid growth in artificial intelligence, wearable and neuro-technologies, BCI technologies are making their way into the realms of gaming, education, the workplace, healthcare, and military applications[7].

The proliferation of BCI as an emerging technology stands to constitute a difficult regulatory challenge for legal systems because it is fundamentally different from existing and familiar

[1] Nita A. Farahany, The Battle for Your Brain, *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology* (St. Martin's Press 2023).
[2] Universal Declaration of Human Rights arts. 12, 18.
[3] Marcello Ienca & Roberto Andorno, Towards New Human Rights in the Age of Neuroscience and Neurotechnology, 13 *Life Sciences, Society and Policy* 5 (2017)
[4] Puttaswamy Judgment, *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1
[5] Jonathan R. Wolpaw & Elizabeth Winter Wolpaw, Brain-Computer Interfaces, *Brain-Computer Interfaces: Principles and Practice* (Oxford University Press 2012).
[6] Jonathan R. Wolpaw et al., Brain–Computer Interfaces for Communication and Control, 113 *Clinical Neurophysiology* 767 (2002).
[7] Rafael Yuste et al., Four Ethical Priorities for Neurotechnologies and AI, 551 *Nature* 159 (2017).

forms of digital and technological information collection. While most digital data collection systems require active user participation whether by tapping a message box, sounding out a spoken command, or reporting information via fingerprint, facial scan, or birth plate BCI information is generated by the brain directly[8]. Brain activity itself (in the form of electroencephalogram (EEG) signals, event related potential signals such as P300 waves, or functional near infrared spectroscopy (fNIRS) signals each can by itself unlock information about a person 's mental state, emotion, focus of attention, or decisional processes[9]. Much of this is implicitly generated with no user intention, meaning "your brain can tell me all sorts of things about you that you 're not consciously telling me.[10]

This unprecedented ability to access an individual 's brain states has resulted in a new and incredibly sensitive sort of information often called neuro data. Unlike personal data, neurodata offers a glimpse into a person 's psychological state. In many ways, this information is similar to computer-based metadata about a human mind. When processed using sophisticated machine-learning algorithms, neural data allows the identification of behavioral trends, emotional predilections, predilections and sensitivities, a process that can be characterized as biometric psychography[11].

The explosion of neurodata reveals important gaps in the current landscape of privacy and data protection law. Existing regulatory regimes (e.g., the GDPR in Europe or the CCPA in California) presuppose a world where persons intentionally disclose readily identifiable personal information with the capacity to exercise a reasonable measure of control over how their data is used. These presuppositions come up short when applied to neurotechnology that takes data directly from the brain. More traditional concepts, such as informed consent, transparency, and data minimization, become less applicable or even meaningless when a person cannot knowingly predict, understand, or determine the mental content that the neurotechnology is using.

Moreover, the application of BCIs and artificial intelligence heralds a host of novel legal and

[8] Fabien Lotte et al., A Review of Classification Algorithms for EEG-Based Brain–Computer Interfaces, *Journal of Neural Engineering* 15, no. 3 (2018).
[9] Lawrence A. Farwell & Emanuel Donchin, Talking Off the Top of Your Head: Toward a Mental Prosthesis Utilizing Event-Related Brain Potentials, 70 *Electroencephalography and Clinical Neurophysiology* 510 (1988).
[10] Nita A. Farahany, The Battle for Your Brain, *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology* (St. Martin's Press 2023).
[11] Organisation for Economic Co-operation and Development, *OECD Recommendation on Responsible Innovation in Neurotechnology* (2019).

ethical challenges, such as brain-to-brain neuro-surveillance in the workplace, where companies could foreseeably track neural activity and cognitive states; the capacity for neural profiling to influence brainwashed individuals; and the potential cyber-intrusions into neural implants that could result in a form of "brain jacking." Such forensic "hacking" of neural implants presents potentially severe challenges to personal autonomy and mental integrity and brings the legal ramifications of these technologies into the domain of human rights and constitutional protection.

In this paper I will argue that, due to the unique nature of neurodata, current approaches to regulation are insufficient and new categories of legal protections neuro rights must be established. Neural information is deeply private, requiring a new paradigm of privacy regulation that accommodates information that is involuntarily acquired and uniquely intimate. Neural information also has the unique ability to illuminate thoughts and characteristics that are typically considered private. As such, I will posit the need for new legal safeguards unique to neurodata in order to prevent its exploitation by neural technologies.

In support of its thesis, the paper takes a five-part approach. Part Two describes the technological basis of Brain-Computer Interfaces, illustrating how neural signals are converted into useful data. Part Three summarizes existing privacy and data protection frameworks, emphasizing the new challenges for informed consent under the GDPR and the CCPA[12]. Part Four analyzes the constitutional and human rights issues presented by neurotechnology, concentrating on mental privacy, freedom of thought, and personal autonomy. Part Five surveys legal challenges on the horizon, including neuro-surveillance, algorithmic control, and security of neural systems. The paper concludes by proposing a legal framework under the concepts of cognitive liberty, mental privacy, and mental integrity, outlining a path forward to preserve cognitive sovereignty in the era of consumer neurotechnology[13].

Technical Foundations and the Anatomy of Neurodata

Therefore, a proper legal analysis of BCIs must be grounded in an understanding of the technology they utilize. BCIs are not just a digital readout of neural activity they are specialized technologies that establish a new pathway of communication between the human brain and

[12] General Data Protection Regulation arts. 5, 6 & 9; California Consumer Privacy Act.
[13] Organisation for Economic Co-operation and Development, *OECD Recommendation on Responsible Innovation in Neurotechnology* (2019).

computers. Through the transduction of electrical or physiological signals produced by neural activity into digital code, BCIs effectively signal computers of information and intentions normally inaccessible to digital computers information regarding our thoughts, feelings, and actions. This novel ability to interconnect the human mind with computing technology creates unique privacy concerns that other digital technologies cannot claim[14].

Our brains are made up of about 86 billion neurons, all of which communicate with each other using electro-chemical signals[15]. When we think, remember something, decide, feel emotions or do physical acts, huge groups of neurons produce electrical activity which can be recorded, monitored and interpreted. Brain Computer Interface systems are developed to do just this. They take data produced by the brain and convert it into meaningful digital information[16]. In general, BCIs are either invasive, semi-invasive or non-invasive depending on the type of data collection used. Invasive systems are those in which electrodes are implanted surgically in the brain tissue and record neural activity directly. These systems are used almost solely for medical purposes, to re-establish communication or motor abilities for patients with severe neurological deficits. Semi-invasive devices like Electrocorticography (ECoG)place electrodes on the surface of the brain below the skull and offers the best compromise between accuracy and surgical risk[17].

However, the most pressing legal issues is the proliferation of non-invasive consumer neurotechnologies. These technologies are often based on EEG measuring electrical activity through sensors placed on the scalp or f NIRS measuring variations in blood oxygen that follow neural activity[18]. They are not invasive, and many are already embedded in products like headsets, earbuds and other smart devices. As neurotechnology becomes more commercially viable and less expensive, its use for constant, consumer-level neural measurement will soon become a part of daily life.

In the past, one of the most prohibitive barriers to reliable non-invasive monitoring of brain activity was the high rate of noise and distortion brought about by recording from the scalp.

[14] Marcello Ienca & Roberto Andorno, Towards New Human Rights in the Age of Neuroscience and Neurotechnology, 13 *Life Sciences, Society and Policy* 5 (2017).
[15] Eric R. Kandel et al., Principles of Neural Science, *Principles of Neural Science* (McGraw-Hill 2021).
[16] Jonathan R. Wolpaw & Elizabeth Winter Wolpaw, Brain-Computer Interfaces.
[17] Niels Birbaumer, Breaking the Silence: Brain–Computer Interfaces for Communication and Motor Control, *Psychophysiology* (2006).
[18] Fabien Lotte et al., A Review of Classification Algorithms for EEG-Based Brain–Computer Interfaces, *Journal of Neural Engineering* 15 (2018).

Neural signals have to travel through a significant layer of both bone and soft tissue before reaching the recording electrodes, and this distorts both the types of signals and their relative amplitude to each other. Recordings are also highly susceptible to noise introduced by eye movements, facial muscle activity, ambient electrical interference, and other physiological signals. Until recently, this made consumer neurosciences applications impractical. Digital filtering powered by artificial intelligence is now able to reverse these effects to a significant extent, allowing for unambiguous interpretation of EEG data.

Once received, these signals need to go through several processes in order to be of usable value. The raw signals are physically amplified, digitized, and filtered with hardware circuits to eliminate unwanted noise signals. Once the signals have been cleaned, more complex computer algorithms, such as Independent Component Analysis (ICA), can be used to separate neural signals from blinks, muscle movements and other electromyograms[19]. After the signals have been cleaned, feature extraction can be performed. This is the process of highlighting a set of features from the neural signals that best represent the brain signal. One typical form of feature extraction measures neural oscillation in several frequency sets. Delta, gamma, alpha, beta, and theta waves are almost synonymous with certain brain functions. Delta waves are related to deep sleep. Theta waves are found during creative thought and memories. Alpha waves are related to relaxed states. Beta waves are related to concentration and active thought. Gamma waves are related to higher mental activity and consolidation of information[20].

A further significant source of neural information is Event-Related Potentials (ERPs), which are transient fluctuations in brain activity that are evoked by a given stimulus[21]. Of recent interest is the P300 wave, which is thought to reflect the brain ‘s response to familiar or meaningful stimuli[22]. That is, the neural signature of the P300 indicates the brain is aware that the individual has seen and recognizes an image, word or concept, even though they are not expressing this awareness behaviorally. The existence of the P300 in a person ‘s neural profile raises serious legal and ethical issues, because this element can be detected without the person ‘s ever having voiced it.

[19] Aapo Hyvärinen & Erkki Oja, Independent Component Analysis: Algorithms and Applications, 13 *Neural Networks* 411 (2000).
[20] Mark F. Bear, Barry W. Connors & Michael A. Paradiso, Neuroscience: Exploring the Brain, *Neuroscience: Exploring the Brain* (4th ed., Wolters Kluwer 2015).
[21] Steven J. Luck, *An Introduction to the Event-Related Potential Technique* (2d ed., MIT Press 2014).
[22] Lawrence A. Farwell & Emanuel Donchin, Talking Off the Top of Your Head: Toward a Mental Prosthesis Utilizing Event-Related Brain Potentials, 70 *Electroencephalography and Clinical Neurophysiology* 510 (1988).

The presence of the machine-learning paradigm in BCI data processing only exacerbates this kind of manipulation. State-of-the-art machine-learning algorithms like Convolutional Neural Networks or Recurrent Networks are capable of discerning implicative patterns within neural data that are undetectable by the human eye[23]. Learning from massive amounts of data, machine-learning algorithms can learn to forecast emotions, attention levels, mental fatigue, stress reac- ions, preferences, and more. This transforms neural data into a complex behavioral profiling far removed from the initial stimulus[24].

This shift has created something that could be referred to as neurodata, a special and highly sensitive category of personal data. Unlike traditional examples, neurodata comes from the nervous system of the human body, and is its hallmark characteristic that it does not arise from an individual actively, and consciously, attempting to do so. sending an email via the Internet, speaking into a microphone, or swiping your fingerprint at a security checkpoint require an action on the part of the individual; by contrast, the generation of neural activity occurs entirely spontaneously. There is no way for a person to will herself to cease generating neural responses exactly as she can will herself to refrain from sharing other types of personal data[25].

The implications of these types of neurodata, legal or otherwise, are made all the more profound when you understand their predictive nature. Where traditional biometric information (i.e. a fingerprint or portrait) aids in confirming whose identity a particular piece of information belongs to, neurodata reveals what that entity is thinking and feeling, how it remembers, and how it perceives and acts on the surrounding environment. With the help of modern computing techniques, institutions could utilize neural information to construct detailed psychological profiles that go far beyond the person's physical and emotional makeup, revealing information about its inclinations, flaws, mental health, etc. (a popular term for this type of information is biometric psychography).

Furthermore, neurodata may also involve new issues related to identification and data protection. New evidence about neural pattern activity indicates that neural information might constitute a very idiosyncratic cognitive signature, so that individuals could be identified with 80-99% accuracy even in the absence of traditional identifying information. As such,

[23] Yann LeCun, Yoshua Bengio & Geoffrey Hinton, Deep Learning, 521 *Nature* 436 (2015).
[24] Marcello Ienca & Roberto Andorno, Towards New Human Rights in the Age of Neuroscience and Neurotechnology, *Life Sciences, Society and Policy* 5 (2017).
[25] Michele Farisco, Kathinka Evers & Jean-Pierre Changeux, Neurotechnology and Human Rights, *Neurotechnology and Human Rights: New Challenges to Human Dignity* (Springer 2022).

traditional anonymization approaches may be insufficient for neuro-data, and the existence of re-identification risks for supposedly anonymous neuro-data raises concerns about surveillance, profiling and long-term data protection[26].

These technological developments make it clear that BCI is not simply the collection of one more type of sensitive data. To the contrary, it offers a new window into the very forces that govern who we are. The real danger of BCIs is the ability not just to record, but to read the dynamic and ongoing activity of the brain: something that current privacy legislation was conceived in ignorance of. That makes it hard to determine whether existing statutes are up to the task of protecting privacy and what additional protective measures might be needed[27].

The Conceptual Crisis in Current Data Protection Law

The unprecedented growth of consumer brain-computer interfaces has revealed a fundamental flaw in modern data privacy and protection law. While a number of expansive legal frameworks including the European Union's General Data Protection Regulation ("GDPR"), and the California Consumer Privacy Act ("CCPA") have been established, these legal regulations were created during a time when people 's private information was readily recognizable as data that they not we voluntarily and consciously entered, clicked, typed, or otherwise generated with some form of intent. Advances in neurotechnology, on the other hand, have made it ever more difficult to keep this assumption intact, as private information can now be obtained through neural activity itself without any clear word from the data subject. This complicates the legal status of data relationships, as the nature of the relationship between a data subject and data controller itself poses a regulatory challenge.

One of the most significant legal questions in many areas will be the distinction between clinical versus consumer neurotechnology: While clinical neural information derived from implanted neurodevices and therapeutic neurotechnologies will presumably be covered by existing stringent healthcare privacy and security regulations, consumer neural data collected by EGG-headphones, neuro-sensing ear buds, gaming peripherals, work monitoring applications, or other devices may not be regulated under healthcare statutes. This may mean that information about a person 's thoughts, feelings, emotions, mind, and perhaps neurological

[26] General Data Protection Regulation arts. 4, 5, 9 & 25.
[27] Rafael Yuste et al., Four Ethical Priorities for Neurotechnologies and AI, 551 *Nature* 159 (2017); United Nations Educational, Scientific and Cultural Organization, *Recommendation on the Ethics of Artificial Intelligence* (2021).

health would be considered unsensitive commercial data rather than sensitive health information under the law.

The drawbacks of the GDPR are particularly clear when looking at its application to neurodata. While the GDPR is considered to be one of the most robust privacy regimes in the world, it was not written with neurotechnology in mind. Under the GDPR, special types of personal data, also called sensitive, or special categories of data are given increased protections. Amongst these are biometric data, and health data, according to Article 9. While the neural data itself would seem to fall easily under the biometric category, the data ‘s descriptive power does not rest in the identification of a person, so much as the characteristics and information about their state of being, in terms of their psychological makeup and behavior tendencies. Modern BCI systems are more and more often used for psychographic profiling, rather than simply confirming an individual ‘s identity. Some processes involving neural data would seem not to benefit from the protections of Article 9, leaving a somewhat undefined category of data more sensitive than many forms of traditional biometric data.

Another similar problem arises in relation to the principle of informed consent, a safeguard which forms part of most modern data protection laws. Under the GDPR, consent must be given freely, be specific, informed and unambiguous. However, this is all founded on the assumption that individuals have an understanding of the nature of the information they are providing and are able to give meaningful consent.

Consent to a use. In the realm of neurotechnology, this assumption appears to be more and more arduous to defend however. Neural reactions are often involuntary, subliminal, occurring deep down and long before the consumer is consciously aware of their existence. A consumer of a neurotechnology product cannot be expected to anticipate every neural pattern that may be produced when that device is used or even foresee how those neural patterns may be summoned up by future artificial intelligence systems. Thus, informed consent becomes less meaningful since the consumer is essentially granting permission to have information collected when the consumer himself is unable to know what the nature, extent, and consequences of that information are.

Data minimization is also hindered by similar issues. Data protection legislation generally requires companies to only collect the minimum data required for a purpose. The principle works in the traditional digital environment, where individual data elements such as a name,

email address or location information are collected discretely. Neurodata, cannot be collected in this manner, as neural signals are everything at once. A BCI collecting data for a particular task, will also collect information about emotion, alertness, stress levels, mental exhaustion and perhaps even neurological health. Since all of this signal resides within a single neural stream, the signals cannot be segmented. Data minimization, again, runs into difficulties when applied to neurodata.

The state of regulation in the United States further conveys the ongoing, multidirectional efforts toward regulation that are occurring in the field of neurotechnology. Unlike in the European Union, where there is a unified, overarching privacy law, the United States has a patchwork of reform achieved at the state level. As the risks of neurodata become better understood, more states are legislating for the protection of neural information. Colorado has become the first state to specify the body-specific nature of neural data by making neural information a category of information that is respected as sensitive. Similarly, California has promulgated an update to their consumer privacy law that described direct measures of activity within a person ‘s nervous system as a category of sensitive personal information. These are positive developments, because they illuminate additional reasons why neural data is so different from other types of personal data; they also suggest that legislation is beginning to recognize that existing privacy regimes will not suffice in the context of neurotechnology.

Nevertheless, the legal protections continue to be incomplete and disjointed across broad swaths of the legal landscape. Existing protections are non-existent or inconsistent at best across geographic boundaries, leaving many consumers uncovered against the commercial utilization of neural data. Additionally, the most robust privacy statutes still rely on a notice-and-consent paradigm that overestimates people ‘s ability to have meaningful control over the information they produce[28]. This assumption is becoming less tenable with technologies that can monitor subconscious mental activity. Neurotechnology exposes a deeper conceptual flaw in our contemporary privacy legal regime: existing devices were designed for governing information transactions, but neural data accesses the very process by which thoughts, feelings, and decisions are formed. Thus, as the field advances, so too must the law in order to protect Mental privacy and cognitive autonomy may need to be brought under a legal framework that

[28] General Data Protection Regulation arts. 5–7.

moves beyond data protection and recognizes the human mind as a separate domain in need of its own legal protection.[29]

Constitutional and Human Rights Dimensions

The advances of neuroscience and the proliferation of brain computer interfaces (BCI) raise issues that go far beyond the scope of data protection and consumer privacy. Neurotechnology has the capacity to not only turn neural signals into data but to enable the recording, understanding, and even manipulation of the neural activity itself. In doing so, it invades fundamental constitutional rights and internationally established human rights. For millennia, the law has assumed there was a place beyond the reach of government authority the mind[30]. While the law and society could exercise regulation of the actions, communications and behaviors of citizens, thoughts themselves had been out of reach[31]. The origan there was and should be no access to the thinking mind the natural removal of the seeing eye, the deaf ear, and the disconnected mind had created an unpopulated yet established sovereign boundary between the individual and the state one from which the ideas of autonomy, freedom of conscience and human dignity had been borne.

Perhaps the most powerful constitutional issue involved in this conversation is governed by the First Amendment to the United States Constitution[32]. While the First Amendment is best known as a safeguard for speech, press, and association, its protections are based on a more fundamental doctrine: cognitive liberty and the individual ‘s control over the flow of information into and out of their mind. This is the very measure on which we depend for democracy and the resulting openness to reason that allows societies to function effectively. This fundamental safeguard to thought has been consistently reaffirmed by the Supreme Court of the United States and is the foundation for the protections afforded by the First Amendment. However, neurotechnology, especially cognitively non-invasive varieties, threaten the very concept of cognitive liberty by bridging the gap in the traditional view of emancipation of thought from speech. BCI technology can, pre-Speech, tap into “feelings, preferences, beliefs, memories, etc.” so that “a person no longer has the opportunity to form a decision to disclose

[29] Marcello Ienca & Roberto Andorno, Towards New Human Rights in the Age of Neuroscience and Neurotechnology, 13 *Life Sciences, Society and Policy* 5 (2017).
[30] International Covenant on Civil and Political Rights arts. 18 & 19.
[31] Universal Declaration of Human Rights arts. 18 & 19.
[32] First Amendment to the United States Constitution.

this information"; in the future, governments and corporations will be able to access our intellectual domain[33].

The Fourth Amendment presents novel challenges as well in the neurotechnology ecosystem[34]. Where law enforcement agents would normally just need to show a warrant or probable cause before infringing upon an individual's privacy rights, the Fourth Amendment embodies the expectation that these burdens must be carried[35]. The Fourth Amendment now acknowledges that privacy is not only a right in physical spaces, but in things in which privacy is reasonably expected. Criminal suspects arguably have this expectation of privacy in their perceptions, cognitions, and internal reactions to the world. The state-of-the-art in brain technology, and the new legal framework that it is engendering, is therefore at a crossroads. With the advent of cloud computing paradigms that introduce closer proximity between neural data and third-party intermediaries, a troubling possibility arises: is neural data that is suddenly more helpless against the reach of the law? The framework of classically-held principles of reasonableness and guided discretion, or of established legal doctrines of third-party disclosures, cannot justify control of the data of the mind and brain. The potential of neural data to cause the law to fall short in protecting cognition argues that neural data must be granted heightened levels of Fourth Amendment scrutiny such as requiring distinctive warrants and heightened privacy measures.

The other major implications of neurotechnology relate to the Fifth Amendment privilege against self-incrimination[36]. The Fifth Amendment normally protects individuals from having to produce "evidence that would itself prove the person 's guilt." Courts have distinguished between physical (biometric) evidence and speech (testimonial) evidence in this context. BCI technology complicates this distinction because neural signals can be both. Neural signals can be directly measured through sensors; they are physical in nature. However, the information extracted from neural signals can contradict the physical source and reflect the person 's actual knowledge, recognition, beliefs, and thoughts. Imagine a police officer using a BCI to discover whether the suspect recognizes an image, phrase, name, place, or object as having some sort of connection to the alleged crime. The defendant 's brain activity may be detected by the sensors,

[33] Marcello Ienca & Roberto Andorno, Towards New Human Rights in the Age of Neuroscience and Neurotechnology, 13 *Life Sciences, Society and Policy* 5 (2017).
[34] Fourth Amendment to the United States Constitution.
[35] Katz v. United States, 389 U.S. 347 (1967).
[36] Fifth Amendment to the United States Constitution.

but what is being revealed by that activity reflects his thoughts, perceptions, and internal experiences. In essence, the evidence is testimonial rather than physiological. Requiring a defendant to produce this kind of subjective knowledge would run counter to the intent behind the Fifth Amendment.

In addition to constitutional law concerns, neurotechnology also presents a host of more pressing issues under the scope of international human rights law. The right to privacy has been characterized by the United Nations as a human right, by which the European Convention on Human Rights ('ECHR') protects 'respect for private and family life', [4] and by which the European Court of Human Rights has 'stretched…the scope of [the] Charter to include…psychological well-being and personal autonomy'. [5] Yet privacy instruments were defined in response to physical observation, personal data gathering and telecommunication surveillance. Neurodata presents a different problem: instead of access to observable conduct, we could gain entry to thoughts and feelings. We could learn everything someone has thought or feared, everything they have wanted or believed, everything they would never have wanted to reveal. We would gain control over their thoughts and feelings and in doing so, we would cease to see human beings as human beings.

The impact of Brain-Computer Interfaces on human cognition underscores that there is an immediate need for new legal protections. Existing constitutional and human rights protections provide a solid foundation, but have originated in a time when direct access to human mental processes was technologically impossible. As life becomes more inundated with Brain-Computer Interfaces, legal protections must adapt and acknowledge that the protection of the privacy of the mind is on par, if not higher, than the protection of the privacy of the home and the privacy of cyberspace. Such protections should include the protection of mental privacy, cognitive liberty, and psychological interference.

Emerging Legal Threats: Brain jacking, Neuromarketing and the Workplace

The commercialization of BC has so radically altered the concerns about neurotechnology from hypothetically deliberated issues to tangible legal and social problems. As these new technologies start being a part of consumer applications, workplaces, healthcare institutions, and even social media, they are engendering shadows of vulnerability that our existing legal systems are neither read nor able to dealing with[37]. In contrast to digital technologies, brain-

[37] Nita A. Farahany, The Battle for Your Brain, *The Battle for Your Brain: Defending the Right to Think Freely*

computer interfaces offer a direct channel between the human brain and computational machines that opens an entirely new front of digital attacks. Therefore, threats to neurotechnology are not only about crime and invasion of privacy anymore but they range from direct compromise of mental integrity, emotional health, and capacity for independent decision-making, to infringement upon physical integrity[38]. Some of the most significant possibilities of the large-scale deployment of BC is include cyber-neurosecurity issues, the promotion of neuromarketing, and increase of neuro-surveillance in the working environment.

One of the most alarming dangers of all is "brain jacking," defined as gaining access to a BCI system through its neural interface and subverting its function. Computer crimes today tend toward stealing information, misappropriating resources, or scamming consumers. Brain jacking represents a different kind of assault, since it targets a technology interfacing with the human nervous system[39]. An effective attack against an implanted or bidirectional BCI could impact neural stimulation, motor control, emotional regulation, and cognition. Even a non-invasive entertainment system or headband is subject to the compromise of received neural data, leading attackers to potentially retrieve extremely sensitive information related to thoughts, feelings, and intentions[40]. These assaults trigger thought-provoking fears about the right to mental self-determination, turning breaches of cybersecurity into infringements of an individual.

Legal liability offers one mechanism to prevent brain jacking, yet the analysis above reveals expensive gaps in today 's legal infrastructure. Product liability laws may or may not, depending on the jurisdiction, offer a remedy when a manufacturer fails to incorporate appropriate Sicherheitsmaßnahmen to prevent cyberinteractions or knowingly sells a product embodying avoidable flaw in terms of cyber defense. So long as a pinched brain giver results in psychological harm, bodily injury, or mental distress, all the manufacturer need show is that the BCI was defectively designed or did not include crucial cybersecurity protections and therefore liability may be successfully brought. Causation, however, would be very hard to demonstrate.2 Given the idiosyncrasies of neural functioning, and the individuality of each braing as, a plaintiff would need the resources to bring a highly technical expert to the table demonstrating unlikely neural effects to show a BCI caused a person 's deviation from the

in the Age of Neurotechnology (St. Martin's Press 2023).
[38] Rafael Yuste et al., Four Ethical Priorities for Neurotechnologies and AI, 551 *Nature* 159 (2017).
[39] Institute of Electrical and Electronics Engineers, *IEEE Brain Neurotechnology Standards Roadmap* (2021).
[40] Nita A. Farahany, The Battle for Your Brain.

expected nitic state. Similar problems bedevil criminal law. The laws on cybercrime were built to criminalize hacking at the server level, not the person. Today, even legislatures lack a direct measure or sentencing enhancement for crimes committed via cyberweapon upon neural technology or the person--a lacuna that needs filling.

In addition to the threat to digital and physical security, expanding markets for neurotechnology have had a hand in the rapid flourishing of a relatively new industry in the marketing realm neuromarketing. This industry is based on using neural data to both analyze and shape consumer decision making. Current marketing practices are based on surveys and important feedback about individual preferences, life experiences, and buying habits in addition to tracking consumer purchases, browsing patterns, and all other behaviors that can be monitored, personal characteristics that are only known as far as each consumer directly reports them[41]. The advent of neurotechnology revolutionizes and expands the reach of this process allowing companies to look directly into conscious minds to observe not just what consumers say they will buy but what they didn't know they wanted measuring instantaneous emotions, attention capture, preferences, desires, and repulsions. It offers these companies a completely new understanding of what makes consumers tick[42].

This legal problem arises if and when neuromarketing crosses over from persuasion into manipulation. Obvious efforts of such sophistication are unlikely to go unnoticed, but thinking machines capable of measuring minute cognitive weaknesses and emotional states on the fly can craft personalized advertising and "think" with targeted consumers when they are already feeling most vulnerable: under stress, fatigued, emotionally compromised[43]. In such cases, the line separating manipulation from consumer force feeding becomes very thin indeed. Consumer-protection laws are targeted at deceptive, fraudulent, and unfair commercial conduct but have not been designed for technologies capable of surveilling the invisible thoughts capes of the mind. Neuromarketing thus raises complex behavioral legal challenges that require consideration of what counts as autonomous decision-making, to what degree it is reasonable to expect and assume human beings take prior advertising "hits, "and how far commercial players should be allowed to influence their behavior from direct access to brain states.

[41] Leon Zurawicki, *Neuromarketing: Exploring the Brain of the Consumer* (Springer 2010).
[42] Rafael Yuste et al., Four Ethical Priorities for Neurotechnologies and AI, 551 *Nature* 159 (2017).
[43] Organisation for Economic Co-operation and Development, *OECD Recommendation on Responsible Innovation in Neurotechnology* (2019).

The workplace is yet another domain where neurotechnology presents a host of significant legal and ethical issues[44]. Employers are beginning to investigate employment applications of neural monitoring devices to promote efficiency and reduce accident rates in the workplace. If neuro-monitoring is implemented in safety-critical industries such as transportation, aviation, mining, manufacturing and other high-risk fields, there is the potential for meaningful benefit through the identification of fatigue, distraction and decreasing attention prior to incidents.[45]

However, the common use of workplace neuro-surveillance is not without danger. The invasive, ongoing monitoring of brain activity provides unprecedented access to information about mental function. Work-related data concerning concentration, mood, agitation, frustration, and cognitive burdensome could be exploited in work performance assessments, and further a basis for motivating promotion, demotion, or discipline. This dominant use of neuro-surveillance would perpetuate an extreme imbalance of power. An employee would risk workplace hardship in the very event that he or she did not acquiesce to neural monitoring during their employment; with the burden of economic dependency, the degree of expressed consent could be artificially false.

Another issue with neuro-surveillance is the risk of discrimination and inequality in the workplace[46]. As companies start to collect brain data, they will be able to find patterns associated with certain cognitive qualities, emotional states, or neurological conditions. While their data might not be used with the intention of discriminating them, employees could be rejected by automatic decision-making if they are just outside of the supposed normal of "healthy, happy and engaged." If the employee is showing signs of stress and anxiety, or even neurodivergence or the beginning stages of a neurological disorder, they might be discriminated against without even having underperformed. This is especially problematic in this context, because since these decisions are made based on complex algorithms, the person being discriminated against might not be able to prove that they were the victim of discrimination[47].

It is these and related concerns about privacy and autonomy that have animated much of the historical debate on lie-detectors and other types of physiological monitoring in the workplace.

[44] Nita A. Farahany, *The Battle for Your Brain* (2023).
[45] European Data Protection Board, *Guidelines on Consent under Regulation 2016/679* (2020).
[46] International Labour Organization, *Protection of Workers' Personal Data* (ILO Code of Practice 1997).
[47] United Nations Educational, Scientific and Cultural Organization, *Recommendation on the Ethics of Artificial Intelligence* (2021).

At present, many legal regimes have begun to acknowledge the limitations of the employers' right to delve into the private mental states of its workers. Neurotechnology 's rapid advances, however, raise the prospect that similar limits will be invoked when it comes to neural data. Advocates interested in maintaining workers' basic, inalienable rights to mental privacy and mental integrity will therefore have to call for safeguards that restrict or ban the broad use neuro-monitoring tools, outside of narrow safety and medical applications[48].

In sum, the potentials for brain jacking, neuromarketing, and neuro-surveillance at work show that the nature of risks posed by the BCI paradigm is much broader than the simple violation of data privacy. This paradigm provides a tool for invasive control of the very space of human thought, sensibility, memory, and choice at a scale that threatens the very foundations of human rights as currently understood. As the boundaries and possibilities of neurotechnology continue to expand, our legal mechanisms and protections must expand with them--not just the shields against neural data espionage, but also the structures that will preserve the values of equality, dignity, autonomy, and individual control over the mind[49].

The Neurorights Revolution: A Blueprint for Future Governance

The problems associated with BCIs demonstrate that current mechanisms of privacy and data protection are no longer enough to protect the individual in the realm of neurotechnology[50]. As shown in previous sections, neurodata is fundamentally different from traditional types of personal information since it is sourced from neural activity and can give information about thoughts, feelings, intentions and cognitive weaknesses[51]. Thus, building just on existing legal regimes or legislating in small steps may not give enough protection. Instead, a more comprehensive change in legal thinking may have to occur, one that recognizes the human mind as a niche of legal protection and that grants rights specifically for this area in the twenty-first century. Such thought pattern is summarized under the rise of the concept of "neurorights," which is the way of framing rights to protect human dignity, autonomy and mental integrity and agency against the ability of neural data to be monitored, understood and

[48] Nita A. Farahany, The Battle for Your Brain, *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology* (St. Martin's Press 2023).
[49] Nita A. Farahany, The Battle for Your Brain, *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology* (St. Martin's Press 2023); Marcello Ienca & Roberto Andorno, supra note 45.
[50]Nita A. Farahany, The Battle for Your Brain, *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology* (St. Martin's Press 2023).
[51] Marcello Ienca & Roberto Andorno, *Towards New Human Rights in the Age of Neuroscience and Neurotechnology*, 13 *Life Sciences, Society and Policy* 5 (2017).

accessed[52].

The discussion of neurorights at a global level has already started to generate changes in legislation. The date of the achievement in Chile was one of the most important moments, I think. In fact, this country became the first in the world to officially protect the use of information created from brain activity within the constitution[53]. There is no more reason to preserve the mental integrity and the neural information as such, since the Chilean Constitution states that is when we protect the mental integrity, neural information, mental states, intellectual activity and inner life of human beings. It is a milestone in rights history as it rejects the characterization of neural information as another personal data category and treats it as a human right. However, it is also a paradoxical achievement because it shows how challenging will be to delimit the regulation of neurotechnology within the narrower limits of medicine or health care. While BCIs will be increasingly present in everyday life products, education, entertainment, jobs, legislation must provide pressure not only in health care but also in other areas[54].

In doing so, I propose that a three-pronged s of neurorights cognitive liberty, mental privacy, and mental integrity can provide a rigorous yet flexible foundation for establishing the necessary limits on neurotechnology while respecting the core patrimony of human liberty and independence. I define cognitive liberty as the right to make autonomous decisions by choosing when and how to use neurotechnology to make neural changes. Such a right would safeguard the liberty of individuals from involuntary neural surveillance, behavioral nudging, or compulsory neural enhancement, and would affirm that people retain the right to freely choose or refuse great technological gifts with no threat of economic exploitation or ideological coercion[55]. In this way, cognitive freedom broadens the old right to Freedom of Thought to include the presence of powerful technologies that could intrude into our mental space.

The second pillar is the protection of mental privacy[56]. The goal of the category of mental privacy is to prevent the unauthorized access of neural information by companies or other

[52] United Nations Educational, Scientific and Cultural Organization, *Recommendation on the Ethics of Artificial Intelligence* (2021).
[53] Chile, Constitutional Reform Law No. 21.383 (2021).
[54] Nita A. Farahany, The Battle for Your Brain.
[55] United Nations Educational, Scientific and Cultural Organization, *Recommendation on the Ethics of Artificial Intelligence* (2021).
[56] Marcello Ienca & Roberto Andorno, *Towards New Human Rights in the Age of Neuroscience and Neurotechnology*, 13 *Life Sciences, Society and Policy* 5 (2017).

entities. This attempt at reform exceeds the goals of privacy rights because those rights only regulate the collection and use of information after it has been collected; mental privacy imperatives aim to bring about stronger protections at the time of data creation. Neural information collects a person 's experiences, personality, memories, emotional state, and cognitive function of the mind, making it more unique and personal than any other collection of personal information. Because of this, the collection of neurodata must be much more constrained than other forms of personal data. Specifically, it should be used solely for the purpose for which it was collected, and no deductions or conclusions should be derived from it that are not relevant to that purpose. This is crucial to avoid the commercialization of human mind using methodologies such as psychographic profiling and behavioral prediction[57].

The third of these fundamental rights highlights the issues of cyber-neurosecurity and the right to mental integrity. As neurotechnology becomes more extensively networked and more closely integrated with digital systems and artificial intelligence networks, the likelihood of hostile external interference with the human nervous system increases[58]. Mental integrity protects a person from such interference in the human brain whether it be through brainjacking, any unsolicited stimulation of neural networks, or malicious interference with brain function similarly to how the law now protects individuals from physical assault or bodily harm. Identification of mental integrity as a fundamental right thus provides a legal claim to the new kind of security threats that existing criminal and civil law may not yet fully address.

While the recognition of neurorights is certainly a significant normative contribution, the governance of neurotechnology will also require practical mechanisms that can operationalize legal rights into protective guarantees. Perhaps the most promising of these is the introduction of edge-computing architectures for consumer neurotechnology[59]. Digital platforms have often relied on cloud-based computing architectures, which require large quantities of information to be transmitted to massively networked storage systems where it is processed. For neurotechnology, this is potentially dangerous, because at this stage organizations are capable of access to and retention of raw neural signals, which in turn encode information that is often highly sensitive and private. Once the information is transmitted to outside databases, they

[57] Organisation for Economic Co-operation and Development, *OECD Recommendation on Responsible Innovation in Neurotechnology* (2019).
[58] Institute of Electrical and Electronics Engineers, *IEEE Brain Neurotechnology Standards Roadmap* (2021).
[59] Institute of Electrical and Electronics Engineers, *IEEE Brain Neurotechnology Standards Roadmap* (2021)

remain in the domain of control and management of the organization[60].

An alternative approach that is also more concerned with privacy would be edge-computing, where the neural data would never leave the user's device. Instead, the device would collect, filter, and decode the data locally, while only the command itself would be relayed to the outside. For example, if a BCI has been used to navigate a digital interface, then the only data that would be sent outward would be some information about the user directions, which icon to select, or how far to move the cursor). The raw neural data would completely stay on the device. This scheme would circumvent many concerns about profiling, inner data collection, data leaks and looming neuro-surveillance[61].

The introduction of these technical protections must be undergirded by international norms and regulatory directives. Governments, regulators, and standards developers need to set privacy-by-design standards, impose mandatory cybersecurity requirements, and prohibit commercial use of neural data. This will ensure the development of neurotechnology in accordance with fundamental human rights, rather than as a commercial product. However, defining the regulatory landscape should not be considered a hindrance to innovation; in fact, it is the foundation on which public confidence in future neurotechnologies can be established.

In the face of the new opportunities created by the development of Brain-Computer Interfaces, we need a paradigm shift in our current understanding of the contexts of law, technology and the human mind. Legal systems and protections that were built in a time when thoughts and mental processes were accessible to nobody and open to external assessment and analysis will be put under strain by neurotechnology. In turn, the law will have to go beyond traditional notions of privacy in the realm of mental processes and construct a new set of rights the protect the integrity of a person 's cognitive functions, their mental privacy and their cognitive liberty. Technological safeguards and arms control negotiations offer a sound starting point for the lasting protection of the human mind in the age of neurotechnology[62]. Cognitive rights might

[60] Nita A. Farahany, The Battle for Your Brain, *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology* (St. Martin's Press 2023).
[61] United Nations Educational, Scientific and Cultural Organization, *Recommendation on the Ethics of Artificial Intelligence* (2021).
[62] Organisation for Economic Co-operation and Development, *OECD Recommendation on Responsible Innovation in Neurotechnology* (2019); United Nations Educational, Scientific and Cultural Organization, *Recommendation on the Ethics of Artificial Intelligence* (2021).

actually provide the most serious human rights challenge of the twenty-first century[63].

Conclusion

The development and commercialization of Brain-Computer Interfaces (BCIs) are among the most significant technological events of the twenty-first century. While these technologies can be unequivocally beneficial to society through applications related to health, communication, adaptation, learning and human-computer interface, they pose profound technological and philosophical challenges to some of the most sacred principles of legal reasoning and decision-making. For centuries, the human mind has been shielded from external causative interference, thus providing natural parameters which safeguard the freedom of thought, the preservation of human dignity and personal autonomy. Neurotechnology is finally transgressing the boundary between mind and computer by collecting, processing and deciphering neural activity in such a way that aspects of human cognition are being transformed from raw bio-electrical signals into transferable digital information.

This paper has proposed that consumer neurotechnology presents a unique legal problem which will not be sufficiently remedied within the scope of current privacy and data protection rules and values. The data obtained from consumer neurotechnology will be neurodata a kind of personal information that is inherently different from other kinds of personal data because it is derived from brain activity and can possibly serve as an indicator of one's thoughts, preferences, memories, intentions, and perhaps even an individual's psychological weaknesses. Increasing capabilities of artificial intelligence systems to predict meaning from neural signals only exacerbate these concerns. Which such neurotechnology incorporated into commercial products, workplaces, entertainment services, and cyber worlds, the prospect of turning the most sacred elements of one's life into data for sale becomes more and more alarming.

The analysis throughout this paper has shown that existing legal frameworks are clearly unsuited to regulating technologies that have the potential to access and utilize subconscious human mental processes. Existing regulatory schemes such as the General Data Protection Regulation (GDPR) and the, the full implications of the California Consumer Privacy Act (CCPA) depend on notions of 'informed consent', transparency and user control which become more complicated in the case of involuntary neural production and when individuals are unable

[63] Marcello Ienca & Roberto Andorno, supra note 37; Rafael Yuste et al.

to comprehend the present and future uses of information, they did not intentionally disclose. Additionally, this research illustrates both the ways that neurotechnology complicates existing constitutional doctrines of freedom of thought, privacy and protection against self-incrimination, and how it reveals shortcomings in international human rights law that were designed pre-neural access.

Apart from the theoretical issue, commercialization of BCIs can give rise to concrete threats that require urgent legal remedies. Threats such as brain jacking, workplace neuro-surveillance, and neuromarketing reveal how neural information can be exploited to compromise human autonomy and dignity. Tampering with the neural system may threaten mental integrity, while advanced behavioral profiling may allow new levels of influence and manipulation. Similarly, neuro-monitoring tools used at the workplace may end up forcing employees to undergo constant cognitive screening; thereby leaving little space between personal cognition and professional productivity. These concerns indicate that neurotech is not a privacy issue, but more fundamentally an issue concerning civil rights, values of democracy, and social justice.

In light of these problems, this paper offers as a potential solution the introduction of nick euro rights, a new set of legal safeguards for the age of neurotechnology. The framework is predicated on three principles cognitive liberty, mental privacy, and mental integrity and aims to shield the neural object from certain uses and misuses while still respecting individual sovereignty over mental activity. Instead of regarding neurodata as individual commodities, the article argues that information based on neural functioning is protected by a different rule, given that neural functioning is intrinsically linked to human selfhood.

Finally, the paper also discusses that legal safeguards are merely not enough, in the absence of proper technological protections. In this sense, the development of privacy-focused architectures exemplified by edge-computation systems that localize neural data processing rather than streaming raw neural signals to remote servers, can give us a viable technical tool to ensure mental privacy. The various regulation proposed by the policy-makers not only anticipates possible misuses, but also promotes technological development to be aligned with human rights values to prevent the development of vast neural surveillance and it will be able to demonstrate the mutual progress of technological development and human freedom.

In the end, we find ourselves at a crossroads where society must decide the future direction of the nexus between law, technology, and the mind. The choices we make today about how we

will safeguard BCI will determine the boundaries of privacy and freedom for future generations. Without intervention, the risk is real that the human mind could fall under new types of surveillance, speculation, and control. Instead, through meaningful neurorights and safeguards, legislators and citizens can choose the empowering route rather than the oppressive one. The mental domain deserves to be protected from incursions no less than an individual ‘s body or home; safeguarding the right to mental privacy is a necessity to uphold human dignity and free will.

References

i. Nita A. Farahany, The Battle for Your Brain, *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology* (St. Martin's Press 2023). (NLSIU Library Catalog)

ii. Marcello Ienca & Roberto Andorno, *Towards New Human Rights in the Age of Neuroscience and Neurotechnology*, 13 *Life Sciences, Society and Policy* 5 (2017).

iii. Rafael Yuste et al., *Four Ethical Priorities for Neurotechnologies and AI*, 551 *Nature* 159 (2017). (brain.ieee.org)

iv. Marcello Ienca, *On Neurorights*, 15 *Frontiers in Human Neuroscience* 701258 (2021). (Frontiers)

v. Sjors Ligthart et al., *Minding Rights: Mapping Ethical and Legal Foundations of Neurorights*, 32 *Cambridge Quarterly of Healthcare Ethics* 461 (2023). (Cambridge University Press & Assessment)

vi. Laurie Pycroft et al., *Brainjacking: The Security and Privacy Implications of Brain–Computer Interfaces*, *IEEE Security & Privacy* (2016).

vii. Marcello Ienca & Pim Haselager, *Hacking the Brain: Brain–Computer Interfacing Technology and the Ethics of Neurosecurity*, 18 *Ethics and Information Technology* 117 (2016). (brain.ieee.org)

viii. Marcello Ienca, *Neuroprivacy, Neurosecurity and Brain Hacking: Emerging Issues in Neural Engineering*, in *Brain-Computer Interfaces: Lab Experiments to Real-World Applications* (2015). (brain.ieee.org)

ix. Organization for Economic Co-operation and Development, *Recommendation on Responsible Innovation in Neurotechnology* (2019).

x. United Nations Educational, Scientific and Cultural Organization, *Recommendation on the Ethics of Artificial Intelligence* (2021).

xi. Institute of Electrical and Electronics Engineers, *IEEE Brain Neurotechnology*

Standards Roadmap (2021).

xii. Institute of Electrical and Electronics Engineers, *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems* (1st ed. 2019).

xiii. General Data Protection Regulation.

xiv. California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100–1798.199.

xv. Colorado Privacy Act, Colo. Rev. Stat. §§ 6-1-1301 et seq.

xvi. Budapest Convention on Cybercrime, Nov. 23, 2001.

xvii. Employee Polygraph Protection Act, 29 U.S.C. §§ 2001–2009 (1988).

xviii. Artificial Intelligence Act.

xix. Universal Declaration of Human Rights, G.A. Res. 217 A (III), U.N. Doc. A/810 (1948).

xx. International Covenant on Civil and Political Rights, Dec. 16, 1966.

xxi. European Convention on Human Rights, Nov. 4, 1950.

xxii. Chile, Constitutional Reform Law No. 21.383 (2021), recognizing protection of brain activity and neurorights.

xxiii. European Data Protection Board, *Guidelines on Consent under Regulation 2016/679* (2020).

xxiv. Federal Trade Commission, *FTC Policy Statement on Unfairness* (1980).

xxv. International Labour Organization, *Protection of Workers' Personal Data* (Code of Practice, 1997).

xxvi. International Labour Organization, *Safety and Health at the Heart of the Future of Work* (2019).

xxvii. European Union Agency for Fundamental Rights, *Getting the Future Right: Artificial Intelligence and Fundamental Rights* (2020).

xxviii. Leon Zurawicki, *Neuromarketing: Exploring the Brain of the Consumer* (Springer 2010).

xxix. Patrick Renvoise & Christophe Morin, *Neuromarketing: Understanding the Buy Buttons in Your Customer's Brain* (Thomas Nelson 2007).

xxx. David G. Owen, *Products Liability Law* (4th ed., West Academic Publishing 2021).