Neuron

CellPress
OPEN ACCESS

Perspective

Beyond neural data: Cognitive biometrics and mental privacy

Patrick Magee,[1] Marcello Ienca,[2,3] and Nita Farahany[1,4,*]
[1]Duke Initiative for Science & Society, Duke University, Durham, NC, USA
[2]School of Medicine and Health & TUM School of Social Sciences and Technology, Technical University of Munich (TUM), München, Germany
[3]College of Humanities, Swiss Federal Institute of Technology in Lausanne (EPFL), Lausanne, Switzerland
[4]Duke University School of Law, Duke University, Durham, NC, USA
*Correspondence: farahany@duke.edu
https://doi.org/10.1016/j.neuron.2024.09.004

SUMMARY

Innovations in wearable technology and artificial intelligence have enabled consumer devices to process and transmit data about human mental states (cognitive, affective, and conative) through what this paper refers to as "cognitive biometrics." Devices such as brain-computer interfaces, extended reality headsets, and fitness wearables offer significant benefits in health, wellness, and entertainment through the collection and processing and cognitive biometric data. However, they also pose unique risks to mental privacy due to their ability to infer sensitive information about individuals. This paper challenges the current approach to protecting individuals through legal protections for "neural data" and advocates for a more expansive legal and industry framework, as recently reflected in the draft UNESCO Recommendation on the Ethics of Neurotechnology, to holistically address both neural and cognitive biometric data. Incorporating this broader and more inclusive approach into legislation and product design can facilitate responsible innovation while safeguarding individuals' mental privacy.

INTRODUCTION

In recent years, the intersection of emerging technology and personal privacy has become a critical legal battleground.[1] The proliferation of digital devices embedded in our daily lives has dramatically increased the volume, variety, and processing speed of personal data collected. This exponential growth offers unprecedented benefits—such as enhanced health monitoring, improved user experiences, and advancements in human-computer interactions—but also raises significant privacy concerns. The ability of these devices to collect and analyze detailed personal information challenges existing legal frameworks designed to protect individual privacy.

Among these privacy-sensitive types of data are those related to neural activities, known as neural data. This includes quantitative measurements of the structure, activity, and function of the nervous system. Consumer-grade neurotechnologies, such as direct-to-consumer brain-computer interfaces (BCIs), present privacy vulnerabilities including unsecured data-sharing channels,[2] ambiguous privacy policies, and susceptibility to malicious hacking.[3] Recent advancements in artificial intelligence, particularly deep learning applied to neural recordings, have further demonstrated the potential to establish privacy-sensitive statistical correlations between neural data and particular mental states.[4] This capability, while beneficial for personalized health and wellness applications, also poses unique challenges to mental privacy,[1,5] potentially leading to unwanted surveillance and manipulation if not properly regulated.

The urgency to regulate mental privacy risks has resulted in a flurry of recent legal and ethical standards worldwide. However, these regulations (see Table S2) often isolate neural data from broader technological trends, failing to consider how other types of data can also infer mental states. Privacy risks are not confined to direct neural measurements; they can also stem from seemingly innocuous sources such as facial expressions, heart rate variability, and social media interactions. The convergence of these data sources with neural measurements through wearable technologies increases the complexity and scope of privacy concerns,[6] calling for comprehensive regulatory and design-based solutions.

This paper proposes a legal and industry approach that expands the definition of neural data to a broader category called "cognitive biometrics." Traditionally, "biometric" data refers to measurable human characteristics used to identify individuals, such as fingerprints or facial recognition. In this paper, we interpret the term more broadly to encompass both traditional biometric data and data collected through "biosensors"—devices that monitor physiological functions of the human body. This category encompasses not only direct neural measurements like electroencephalography (EEG) and magnetoencephalography (MEG), but also other physiological and behavioral data that can infer cognitive, affective, and conative mental states (hereinafter "mental states"). While the terms "cognitive biometric data" and "cognitive biometric information" are often used interchangeably, with "information" typically referring to data that has been structured and processed to reveal cognitive insights, this paper uses "cognitive biometric data" to maintain

alignment with existing legal language, as documents like Convention 108 do not consistently distinguish between the two terms.[7] And while cognitive biometric data can be collected from both consumer and medical devices, and in both everyday and healthcare settings, the primary focus of this paper is on closing the gap in protections for data collected outside traditional medical or healthcare contexts, where existing privacy laws, such as the United States' Health Insurance Portability and Accountability Act (HIPAA), may not fully apply. By adopting a more inclusive approach to data types that can be used to infer mental states, this paper aims to bridge current gaps in privacy protections and anticipate future technologies advances. This proposed framework advocates for enhanced consumer privacy laws and technological standards that ensure individuals can benefit from these innovative technologies while maintaining robust mental privacy protections.

COMMERCIAL NEURAL AND MENTAL DATA COLLECTION PRACTICES AND LEGAL DEVELOPMENTS

Current industry practices on the collection and use of cognitive biometrics

Neurotechnology comprises "devices and procedures used to understand and/or influence, access, monitor, assess, emulate or modulate the structure and function of the nervous system," (according to the UNESCO draft, p. 4)[8] QA allowing users to interact with virtual environments, quantify their mental states, and control physical objects.[9] With an exponential increase in the filing of BCI patents,[10] and with some consumer-grade neurotechnology companies already boasting hundreds of thousands of users,[11] the collection of neural data is becoming increasingly mainstream. As major technology companies move to embed neural sensors into everyday devices, like earbuds[12,13] and wristbands,[14] this market is projected to grow from $9.8 billion in 2022 to a projected $17.1 billion in 2026.[15] As neurotechnology becomes integrated into everyday consumer products, they join a broader category of biometric data collection devices that raise similar concerns about privacy and ethical use. Biometric data, traditionally used to identify and verify individuals through measurable human characteristics like fingerprints or facial recognition, now encompasses a broader range of data collected by various categories of devices.[16] Biosensors, which monitor physiological functions such as heart rate, brain activity, and eye movements, are increasingly used not only for authentication but also to infer mental states. These biosensors are embedded in a wide array of consumer Internet of Things (IoT) devices—a network of interconnected gadgets that collect and exchange data, often without human intervention. As neurotechnology becomes part of this broader ecosystem, brain sensors used in these devices are just one of many biosensors contributing to these inferences about users' brain and mental states.

As more devices, including XR systems and fitness wearables, incorporate biometric sensors, the implications for privacy and mental health become more pronounced. These devices, such as augmented reality (AR) glasses, virtual reality (VR) headsets, and mixed reality (MR) products,[17] increasingly collect biometric data to gain insights about users' brains and mental states, such as monitoring heart rates to assess stress levels[18] and using eye tracking data to understand intentions and cognition.[19,20] Companies like Meta,[21] Sony,[22] Microsoft,[23] and Apple[24] are driving this trend, contributing to a global XR market expected to grow from $54.58 billion in 2024 to $100.77 billion by 2026.[25] Similarly, fitness wearables like Fitbit[26] and Apple Watch,[27] which monitor heart rate and other physiological functions, are regularly used by over one in five Americans[28] and are projected to expand from an estimated global market size of $62.03 billion in 2024 to $290.85 billion by 2032.[29]

While the collection and analysis of data related to brain and mental states offer significant consumer and medical benefits,[30] they also raise profound ethical concerns about mental privacy.[2] The term "cognitive biometric data," introduced on page 5 of the first draft of the UNESCO global standard on the ethics of neurotechnology[8] drafted collectively by AHEG members, including authors Farahany and Ienca, provides a broader framework for understanding these risks. This framework is essential because data about brain and mental states of individuals, although valuable for various consumer and medical applications, has the potential to reveal intimate information about users. Cognitive biometric data, which includes neural data, is uniquely sensitive because it "provide[s] deep insights into the pre-behavioral processes that underpin" our cognitive, affective, and conative functions (see page 22 of the UNESCO draft).[8] Like ink on paper that conveys meaning through specific arrangements, cognitive biometric data gain "semantic value"[4] when analyzed to reveal patterns corresponding to mental states or intentions. Raw data such as EEG signals, heart rate variability, or eye-tracking movements initially have no intrinsic meaning, but when processed by sophisticated algorithms, they can be used to infer an individual's mental states, emotions, or intentions, much like how words on a page acquire meaning through context. As the UNESCO draft observes, "the complexity and sensitivity of cognitive biometric data also arise from its ability to capture metacognitive aspects such as self-awareness and introspection." Consequently, these data can reveal detailed personal information "even when collected for unrelated purposes" (page 22 of the UNESCO draft).[8]

Research has demonstrated the ability to predict highly personal traits using EEG, eye-tracking, and heart rate data with remarkable accuracy. These traits include sexual orientation,[31] personality traits,[32] drug use,[33] and mental health conditions[34] (Table S3). When combined with contextual information, such as the user's location or visual field, cognitive biometric data can reveal responses to environmental stimuli. For example, EEG data can reveal whether a user finds a stimulus familiar,[35] eye-tracking data can pinpoint what captures their attention,[36] and heart rate data can measure emotional arousal.[37] This technique, termed "biometric psychography" by Brittan Heller,[38] has even been employed to uncover sensitive information such as proxies for users' PIN numbers and bank account details,[39] romantic attractions,[40] and skill levels in various tasks.[34]

These concerns are compounded by lax industry practices concerning the collection, storage, use, and sale of cognitive biometric data. A recent white paper by the Neurorights Foundation revealed that all thirty neurotechnology companies they reviewed retained broad rights over the neural data they

collected.[41] In our review of the privacy policies of seventeen BCI, XR, and fitness wearable brands, we found that all the BCI and fitness wearable companies indicated that they collect cognitive biometric data from users in at least some circumstances. Additionally, five of the six XR companies either explicitly collect these data or have vague privacy policies that appear to permit its collection (Tables S4–S6). For examples, Sony's privacy policy states that collected information "may include … [i]nformation about the device you are using, any connected peripherals (such as controllers and VR headsets) and how you have configured them"), a broad category that could encompass eye tracking data collected from its VR headset.[42] Only Magic Leap explicitly guarantees that biometric information is processed on their Magic Leap 2 device by default and is never collected by the company[43] (Tables S4–S6). Aside from Magic Leap,[43] all the privacy policies we reviewed include the right to collect contextual data such as location, social media information, and application usage, which could be used to infer consumers' cognitive states in response to their environment (Tables S4–S6). Most companies provide little information about how the data they collect is stored. Of the companies whose privacy policies we reviewed, only Apple explicitly states that they encrypt biometric data in a way that prevents even its own employees from accessing it[44,45] (Tables S4–S6). The remaining companies vary widely in their guarantees. For example, Meta's privacy policy offers virtually no insight into their data storage practices.[46] While six companies claim to use encryption for some types of data, only Emotiv clearly indicates that this includes biometric data,[47] and none mention that the encrypted data are inaccessible to the company and its employees (Tables S4–S6). Other companies offer only cursory descriptions of their security measures, typically affirming that they "seek to maintain appropriate technical and organizational security measures that conform to industry standards"[42] (Tables S4–S6). These limited disclosures provide consumers with little assurance that sensitive insights obtained from their cognitive biometric data will be kept confidential.

Although companies often justify the collection and centralized storage of data with legitimate purposes—such as freeing up local storage and allowing users to access their data from multiple devices—these purposes are frequently defined broadly, enabling many alternative uses of the data that may be only tangentially related to the functioning of the company's products. Instead of specifically delineating how biometric data are used, most of the reviewed companies give wide-reaching purposes like "providing the Services"[48] or "performance management and product enhancement,"[49] which could encompass many unanticipated uses (Tables S4–S6). Some of the purposes outlined by the companies, like HTC's goal "to understand you and your preferences," could potentially be interpreted to authorize the decoding of mental states from cognitive biometric data.[50] Six companies (HTC, Meta, Microsoft, Sony Interactive Entertainment, Samsung, and WHOOP) explicitly state that they may use personal data for marketing purposes, with Samsung and WHOOP indicating that this applies to biometric data[51,52] (Tables S4–S6).

Moreover, since de-identified and aggregate data are not considered personal data under most privacy regulations, companies often do not need to obtain consumer consent before using these types of data for various purposes. When disclosed, these purposes are often vague: for instance, Emotiv and Muse state that they share aggregate data for research purposes, without specifying the aims, background, or underlying ethical principles of this research.[48,49]

Many companies, including Meta,[46] Microsoft,[53] and WHOOP,[52] explicitly state that they do not sell users' personal data, including cognitive biometric data (Tables S4–S6). However, under regulation like the California Consumer Privacy Act (CCPA), a claim not to sell personal data does not preclude companies from using that data to target users with advertisements,[54] as these three companies explicitly reserve the right to do.[52,53,55] These statements also do not restrict the sale or use for advertising of aggregate or de-identified data, which are not classified as personal data. Among the reviewed companies that collect biometric data, nine indicate that they share de-identified or aggregate data with third parties, while none of the others clearly state that they do not (Tables S4–S6). Consequently, these companies provide consumers with no guarantee that sensitive insights derived from their biometric data will not be sold, shared with unscrupulous third parties who may re-identify the data, or used in ways inconsistent with their interests or values.

Even de-identified or aggregated, cognitive biometric data can still pose risks to mental privacy. When such data are combined with other data sources, there is a potential for re-identification or for sensitive inferences to be made about individuals' mental states. This risk is especially concerning when de-identified data are aggregated and shared for purposes such as marketing or product development. Our proposed framework emphasizes that cognitive biometric data—whether de-identified, aggregated, or not—should be subject to heightened protections, recognizing the unique risks it poses when misused. This includes stricter controls over how such data can be used, shared, or repurposed, ensuring that even non-identifiable cognitive biometric data are handled with care to protect individuals' mental privacy.

As these industries grow and the collection of personal data expands, scholars and policymakers have increasingly called for more robust protections for raw neural data.[56] But most efforts to date have focused on the collection of neural data from neurotechnology devices. This approach may be both overspecified and underinclusive in ensuring the ethical collection, processing, transmission, and storage of information relating to the nervous system and mental states. A broader framework that holistically addresses cognitive biometric data is needed to comprehensively tackle these concerns.

Existing consumer privacy and biometric laws pertaining to neural and cognitive biometric data

Given the growing ethical concerns and legal developments surrounding the collection and use of cognitive biometric data, it is crucial to examine how existing consumer privacy laws address these issues. In recent decades, dozens of countries, states, and international organizations have passed general consumer privacy laws that limit the ability of private corporations to collect users' data (Table S1).[57] These legislative efforts reflect

increasing public demand for privacy protections, particularly for highly personal data.[58,59] In addition to giving consumers rights over any data associated with their identity—such as the right to access, correct, and delete collected data—most laws also provide additional protections for "special categories of personal data" or "sensitive data" (our term henceforth) that could "could create significant risks to the fundamental rights and freedoms" (General Data Protection Regulation [GDPR], Recital 51[60]). While legal definitions vary, sensitive data often include information related to one's "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual orientation and sex life, and biometric and genetic data."[61]

Until recently, few if any of these general consumer privacy laws specifically addressed whether neural and cognitive biometric data are considered "sensitive" data. The CCPA, for example, defines sensitive data to include government identifiers, financial information, precise geolocation, communication contents, genetic and biometric data, and information about health, sex life, sexual orientation, race, religion, and union membership (CCPA, 1798.140(ae)[54]). While neural data may qualify as a type of biometric data under certain privacy regulations (Table S1), the CCPA's protections are limited to biometric data that "can be used, singly or in combination with each other or with other identifying data, to establish individual identity" (CCPA, 1798.140(c)[54]). This means that neural data might be treated as sensitive when used for identification purposes,[62] but not when non-identifying neural data are used to infer a user's mental state. A similar concern arises with the Act's definition of health data, which extends to "personal information collected and analyzed concerning a consumer's health" (CCPA, 1798.140(ae)(2)(B)[54]). This definition may exclude biometric data, such as eye tracking data in VR headsets, that is not typically collected or used for health purposes. S.B. 1223, currently under consideration in the California Senate, seeks to address some of these concerns by explicitly classifying neural data as a category of sensitive data under the CCPA, though its scope extends only to information "that can be processed by, or with the assistance of, neurotechnology" (S.B. 1223, Sec. 3[63]).

Biometric laws like Illinois's Biometric Information Privacy Act (BIPA) tend to be even more restrictive. BIPA, for example, extends protection only to a consumer's "biometric identifier[s]," narrowly defined as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" (BIPA, Sec. 10[64]). Although case law has broadened this protection somewhat—for example, to cover facial geometry scans taken from photographs[65,66] or captured for purposes other than identification[66,67]—it remains doubtful whether the law, even when broadly interpreted, covers biometrics such as EEG, heart rate, and several types of eye tracking data, especially when these are not used for identification.[66] These laws are often overspecified and underinclusive, failing to protect comparably risky data categories due to their narrow language.

Recognizing a gap in existing general privacy laws' ability to adequately protect mental privacy, at least twelve countries, regions, and international organizations have proposed or passed new laws, charters, or standard-setting documents since 2018 (Table S2). With lobbying support from the US-based Neurorights Foundation, Chile became the first country in 2021 to codify protections for "brain activity" and data derived from it into their constitution.[68,69] In 2023, the BCI company Emotiv was compelled to delete EEG data it had collected on a former Chilean senator as a direct consequence of Chile's new legislation.[70,71] In the United States, the state of Colorado passed a 2024 law amending the Colorado Privacy Act to protect "data generated by the technological processing, measurement, or analysis of an individual's biological, genetic, biochemical, physiological, or neural properties, compositions, or activities or of an individual's body or bodily functions."[72] However, lobbying efforts narrowed the law's initial broad definition of "biological data" to include only data used for identification,[73] significantly limiting the protections for cognitive biometric data, which can reveal highly personal insights without being used for identification purposes.

The majority of these mental privacy laws, charters, and documents have adopted narrow definitions of neural data, focusing primarily on information obtained directly from the nervous system (Table S2). While these legal approaches are crucial for protecting data directly tied to brain activity, they often exclude broader categories of cognitive biometrics derived from non-neural sources, such as heart rate variability, eye-tracking data, and behavioral patterns. These exclusions mean that many forms of data capable of being processed to infer mental states are not covered, leaving significant gaps in mental privacy protections.

Existing laws such as the EU GDPR[60] and CCPA[54] provide baseline protections for personal data, including neural and cognitive biometric data. However, these protections often fall short of addressing the unique risks associated with data collected outside traditional healthcare settings. Our proposed framework aims to bridge this gap, focusing on enhancing protections for data gathered through consumer devices, where current privacy laws, like HIPAA, may not apply. While the emphasis is on consumer devices, the principles we propose can also inform the protection of data from medical devices in both clinical and non-clinical environments.

General data protection laws mandate consent, data minimization, and purpose limitation, but these measures are typically broad and flexible, allowing for unintended uses of neural and cognitive biometric data. For example, the broad consent permissible under general data protection laws may not provide individuals with a full understanding of how their neural and cognitive biometric data might be used, including potential inferences about their mental states. This issue is further complicated by the fact that many current mental privacy laws, such as those recently enacted in Chile, are primarily concerned with direct brain activity data, leaving other forms of cognitive biometrics, particularly those derived from non-neural sources, less likely to be protected (Table S2). Classifying neural and cognitive biometric data as sensitive data becomes crucial here, as it mandates explicit consent for each specific use, ensuring individuals are fully aware of and agree to the precise ways their data will be used.

Additionally, while general data protection laws enforce data minimization and purpose limitation, they often permit the

repurposing of data for compatible uses without requiring new consent. This flexibility may not adequately protect neural and cognitive biometric data, which can reveal deeply personal and intimate insights. However, if these biometrics are classified as sensitive data, the laws impose stricter limitations on data processing, ensuring that data are only collected and used for the specific purposes for which explicit consent has been given. This tighter control minimizes the risk of data being repurposed in ways not explicitly agreed to by the data subject, providing stronger protection against misuse.

Finally, while general data protection laws mandate basic security measures, these might not be robust enough for neural and cognitive biometric data, which is particularly vulnerable to re-identification and the extraction of sensitive information from even anonymized datasets. Sensitive data protections require enhanced security protocols, such as stronger encryption and more rigorous access controls, precisely because of the higher risks associated with these types of data. By classifying neural and cognitive biometric data as sensitive data, legal frameworks ensure that the highest levels of protection are applied, addressing specific vulnerabilities and safeguarding individuals' mental privacy against unauthorized access and misuse. Recognizing these gaps, some countries have begun to take more comprehensive approaches to protect neural and cognitive biometric data.

Several countries have passed laws or charters taking a more comprehensive approach to protecting neural and cognitive biometrics data, while others are similarly moving to expand their definition of biometrics for purposes other than identification. In 2022, for example, Brazilian legislators introduced an amendment to the Brazilian General Data Protection Law (LGPD) to protect data collected "directly or indirectly" from the "central nervous system."[74] The Mexican Charter of Digital Rights similarly gives privacy protections to data "obtained directly or indirectly through the activity patterns of neurons."[75] In Kenya and Armenia, biometrics laws include physiological or biological data used for any purpose, not just identification,[76,77] and several countries' definition of sensitive data includes mental or psychological health data, which could possibly be construed broadly to include information about mental states (Table S1). In the United States, the Federal Trade Commission (FTC) issued a recent policy statement in which it defined biometrics as "data that depict or describe physical, biological, or behavioral traits, characteristics, or measurements of or relating to an identified or identifiable person's body"[78]—a definition broad enough to likely include all cognitive biometrics linkable to a specific individual, in addition to data such as photographs often excluded from biometric laws.[66] This policy statement signals that the FTC will pursue action against companies that mislead consumers about their collection of biometric data or fail to mitigate harms and risks associated with the collection of these data.[79]

In Europe, Article 4(1) of the GDPR[60] and the CJEU Cases (Breyer[80] and Nowak[81]) consider data related to human brain and mind to be personal data if it can single out the data subject at stake. However, these data may not necessarily be considered sensitive unless it is related to one of the explicitly enumerated categories of sensitive data under Article 9(1) of the GDPR (e.g., data related to health, political opinions, sexual orientation, etc.).[60] This may even be the case if the data can be used to infer highly personal mental states not related to these categories, such as cognitive biometric data correlated with consumer preferences or emotional states. While the 2024 AI Act's classification of emotion recognition algorithms as "high risk" provides additional protections for some types of cognitive biometric data, these protections do not appear to extend to the decoding of non-affective mental states such as cognitive and conative states (AI Act, Article 6(2) and Annex III[82]).

Table S1 lays out the surveyed approaches to this issue.

OUR PROPOSAL

Defining cognitive biometrics

The limitations of existing definitions of neural data in law may at least in part be attributable to the mismatch between the scientific categorization and the legal interests at stake. When medical or scientific terms like "neural data" are imported into law, definitions are often drawn directly from a healthcare or scientific setting where the focus is on diagnosing and treating patients or for ensuring precision in research.[83,84] However, in legal contexts, the purpose extends beyond identifying and treating conditions to creating clear boundaries around personal data to protect rights such as mental privacy and cognitive liberty.[85] By relying on a narrow scientific definitions, existing laws have often failed to protect other categories of information, like heart rate or eye tracking data, which may not be directly related to neural data scientifically but pose similar privacy risks.

This overreliance on scientific definitions is especially evident in recent legislation, such as in Colorado, where two bills regulating biometric data were introduced at the start of 2024 and have since passed. Colorado's H.B. 24-1058 amended the Colorado Privacy Act to classify "biological data," including neural data, as a type of sensitive data.[72] In its Legislative Declaration, H.B. 24-1058 emphasizes that neural data are "extremely sensitive" because they "can reveal intimate information about individuals, including information about health, mental states, emotions, and cognitive functioning." While this rationale applies equally well to cognitive biometrics like eye tracking data, H.B. 24-1058's sensitive data protections extend only to "information that is generated by the measurement of the activity of an individual's central or peripheral nervous systems" and to non-neural biological data only when used for "identification purposes."[72] Similarly, H.B. 24-1130 restricts protections to biometrics that "can be processed for the purpose of uniquely identifying an individual"[86]—a definition that aligns with the two most recent entries in the National Institute of Standards and Technology (NIST) Computer Security Resource Center's glossary[87] but fails to account for privacy harms unrelated to identification, such as disclosure of non-identifying personal information. In each case, the undue weight given to technical definitions has led to the unequal application of legal principles to equally risky categories of data.

Focusing narrowly on specific technologies or data sources, rather than on the broader category of cognitive biometrics, results in underinclusive legal protections. Existing privacy proposals often target specific data sources—such as eye tracking data or facial recognition—rather than addressing the broader class of data capable of inferring mental states.[88–90] While

some proposals, like those from Heller,[38] Spivack and Berrick,[91] and McGill[92] have attempted to expand the scope, they often remain limited to specific technological contexts like immersive technologies, which comprise only a subset of devices using cognitive biometrics.

We argue that the increasing convergence of technologies enabling inferences about brain and mental states calls for a technology-neutral approach. Adopting a more expansive term like cognitive biometrics would allow regulators to treat similar data alike based on inferences they enable and the risks they pose to mental privacy. Cognitive biometrics, as used here, encompasses data from both neural sources and other biosensors that can be processed to infer cognitive, affective, and conative states—collectively referred to as mental states. Where "cognitive" refers specifically to processes related to knowledge, understanding, and thinking, "affective" pertains to emotions and feelings, and "conative" involves desires, volition, and related behavioral intentions.

To guide future policy developments going forward, we propose the following definition of cognitive biometric data, a version of which was recently also included on page 5 of UNESCO's initial draft of a Recommendation on the Ethics of Neurotechnology:

> Cognitive biometric data: "Neural data, as well as other data collected from a given individual or group of individuals through other biometric and biosensor data," which could "be processed and used to infer mental states."[8]

This definition includes direct measurements of nervous system activity, such as EEG and MEG,[93] as well as data from other biosensors, like heart rate and eye tracking, that can be processed to infer mental states. This broader and more inclusive approach ensures comprehensive protection of mental privacy across technologies, regardless of the specific devices or methods used. While the definition of cognitive biometric data shares similarities with the definition of "mental data," which is defined as "any data that can be organized and processed to infer the mental states of a person, including their cognitive, affective, and conative states,"[94] cognitive biometric data specifically emphasize the biometric and biosensor origins of the data used to infer mental states, which provides a clearer and more actionable legal standard.

A potential objection to this approach is that the broad scope of cognitive biometrics could complicate legislation. While neural data are a specific category tied to neurotechnologies, cognitive biometrics encompasses various biological signals and devices. However, this challenge is neither insurmountable nor unique, as biometric laws regulating identification data face similar ambiguities, focusing on inferences about identification rather than specific technologies. For data types that do not clearly enable inferences about mental states, regulators can issue guidelines to clarify their inclusion or exclusion under law.

This approach also offers a practical way to update existing legal frameworks to address novel concerns about mental privacy. Instead of relying on private actors to adopt norms or creating new legislation, it would allow existing privacy or biometrics laws to be updated to include cognitive biometrics. This could be done by revising the definition of sensitive data in consumer privacy laws to explicitly include cognitive biometrics, using the provided definition or a suitable variation. Alternatively, broader definitions of biometrics, like those adopted by the FTC,[78] Kenya,[76] and Armenia,[77] could be used. While the former approach is more tailored to protecting mental privacy, the latter's legal precedence may facilitate easier adoption.

Of the 193 member states of the UN,[95] a clear majority have adopted consumer privacy laws addressing sensitive data.[96] However, some countries and regions lack such laws,[96] and many US states do not have existing consumer privacy laws at all.[97] For jurisdictions without these laws, we propose adopting a privacy "floor" to protect mental privacy. This "privacy floor" establishes a baseline level of protections for mental privacy, ensuring that regardless of jurisdiction, basic standards are met to safeguard individuals' cognitive biometric data. This approach would align with the four categories of protections we outline below, providing a uniform minimum standard that can be tailored to specific cultural and normative differences across the globe.

A privacy "floor" for legislative protections of cognitive biometrics

Our proposed privacy floor captures the essential features of existing consumer privacy laws that govern sensitive data. Despite their differences, these laws exhibit striking consistency in four key areas: informed consent, data minimization and purpose limitation, data rights, and data security. The International Association for Privacy Professionals' (IAPP) Global Comprehensive Privacy Law Mapping Chart surveyed the 23 countries, US states, and international bodies, and found the following:

(1) Informed consent: 17 jurisdictions promote informed consent by both imposing notice/transparency requirements and requiring opt-in consent before processing sensitive data (or, in the case of Singapore, before processing any personal data, subject to specified exceptions).[57,98]
(2) Data minimization and purpose limitation: 22 jurisdictions require companies to limit data processing to specified purposes and to minimize data collection to what is necessary for these purposes.[57]
(3) Data rights: 22 jurisdictions grant consumers specific rights to access, correct, and in some circumstances delete personal data.[57]
(4) Data security: All 23 jurisdictions impose security requirements on the storage of personal data, such as the GDPR's mandate for "appropriate technical and organizational [security] measures" (GDPR, Art. 32(1)[60]).[57]

These principles establish a high baseline of consumer privacy.

- Informed consent ensures consumers are aware of and agree to how their data are collected and processed.
- Data minimization and purpose limitation require companies to collect and process only the data necessary for specified purposes.
- Data rights provide consumers with ongoing control over their data, allowing them to monitor and modify it as needed.

- Data security ensures that data are protected against unauthorized access and misuse.

We propose that these four principles serve as a privacy floor for policies governing the collection, storage, and use of cognitive biometric data, reflecting the best practices of existing privacy laws. This baseline set of standards would protect consumers' mental privacy while allowing for additional context-specific safeguards as needed.

Our privacy floor is intended primarily for lawmakers to evaluate and update existing regulations and to guide new legislation that aligns with global standards. It also serves as a guide for corporations to align their data governance with ethical and legal standards, ensuring consumers that their data will not be misused.

This privacy floor is broad and technology neutral, applying to various technologies that enable the collection and processing of cognitive biometric data. Below, we outline how these principles can be implemented in law and industry privacy policies specifically for cognitive biometrics.

Informed consent

Implementing informed consent for cognitive biometrics involves two major shifts. First, it requires moving from an "opt-out" model, where blanket consent is presumed, to an "opt-in" model where explicit, affirmative consent is obtained before processing certain types of data. This shift has been proposed for BCIs,[99] XR headsets,[90] and fitness wearables.[100] Implementing dynamic consent mechanisms, where users can modify their consent choices in real time as their preferences and context evolves, is also crucial.[101] Second, it would require increased transparency across several dimensions of data processing. Specific transparency measures for cognitive biometrics include clarifying where, by whom, why, and how data are processed and stored,[2,91] disclosing security measures,[2] providing visibility into the design and functionality of AI systems,[90,99] and improving data and technology literacy.[102] These measures aim to rectify the current reliance on click-through consent forms that often lead to uninformed consent.[103]

Data minimization/purpose limitation

Data minimization is a key privacy safeguard for cognitive biometrics, particularly in the context of BCIs,[104] fitness wearables,[105] and immersive technologies like XR headsets.[91,106] While data minimization often focuses on the quantity of data collected,[107] cognitive biometrics requires special attention to the type of data collected. Since raw cognitive biometric data are correlated with sensitive information unrelated to the purpose of data processing (Table S3), data minimization may involve collecting only inferences from cognitive biometric data, or altering the raw data to remove identifying or sensitive features.[108,109] Apple Vision Pro collects eye tracking data only related to "what you select, not what you are looking at."[110] These methods support purpose limitation by tailoring data collection to the specified purpose. However, minimizing data in neural interfaces is challenging due to the difficulty in distinguishing purpose-specific signals from the vast array of underlying brain activity. This complexity necessitates sophisticated tools and techniques to accurately filter and process data while protecting user privacy, such as the Brain Computer Interface Anonymizer, a proposed device to selectively filter data to remove privacy-sensitive information.[111]

Data rights

Rights to access, correct, and request erasure of collected data have been proposed for BCIs,[2] immersive technologies,[91] and fitness wearables.[91] These rights are particularly relevant to the inferences companies extract from cognitive biometrics rather than to the raw data itself. For example, the right to correct data may apply more meaningfully to correcting faulty inferences about a consumer than to correcting raw biometric data. While our privacy floor encompasses the general data rights codified in consumer privacy laws, consistent with the right to cognitive liberty,[1] other proposals advocate for more specific rights such as neurorights[85] or rights specific to domains like extended reality.[92] These specific rights could build upon the privacy floor.

Data security

To implement data security, companies should adopt the most effective and practical encryption methods for the relevant context and category of cognitive biometric data. For BCIs, discussed encryption methods include homomorphic encryption,[112,113] blockchain,[114] secure multiparty computing,[113,115] and differential privacy,[114] with the latter also proposed for eye tracking data[116] and wearable devices.[117] Although not encryption per se, federated learning is noted for limiting access to cognitive biometric data by keeping it on users' devices.[114,118] More broadly, keeping biometrics on users' devices, rather than on company servers (i.e., edge processing) is often mentioned as a means to mitigate privacy concerns.[38,91] While not all of these security methods may be commercially practical—for example, Xia et al. note that encryption methods like homomorphic encryption are "very computationally intensive" and "may not be suitable for real-time online BCI systems"[113]—companies should aim to provide the highest reasonable standard of security given the relevant constraints.

As formulated, these four principles do not require any specific product design features. Nevertheless, we propose that these principles may be effectively implemented in conjunction with a "privacy by design"[119] or "data protection by design and by default" (GDPR, Art. 25[60]) framework for cognitive biometrics. According to this framework, raw cognitive biometric data should by default either be processed on the edge or end-to-end encrypted. These requirements would provide consumers with a substantive assurance of privacy, aligning with the principles discussed.

Edge Processing

> "Edge processing" involves processing data close to its source, such as on a smart device or a local gateway.[120] With respect to cognitive biometrics, the most pertinent form of edge computing involves processing data directly on-device (often termed "ultra-edge")[121] or on proximate wearables, smartphones, or personal computers.

Edge processing of raw cognitive biometric data aligns with three of the four principles constituting our privacy floor:

- Data minimization and purpose limitation: By processing raw data locally, edge computing reduces the need to transfer data to central servers, minimizing the amount of

data collected and stored. It ensures that data collected for one purpose are not repurposed for another.
- Data rights: Users maintain greater control over their raw data, as it remains on their personal devices, allowing them to manage security and storage directly.
- Data security: Keeping raw data on the edge limits the risk of breaches that could occur if these data were stored on central servers.

By shifting raw data processing to proximate, user-controlled devices, edge processing allows applications to use cognitive biometrics without exposing sensitive raw data to corporate servers.[122] This gives users greater confidence that their raw cognitive biometric data will not be exposed or misused.

Edge processing is well suited to the IoT environment in which most cognitive biometric devices operate. Many devices already use edge processing due to its efficiency, speed, and privacy benefits[122,123] (Tables S4–S6). For example, devices like Apple Vision Pro and Magic Leap 2 process eye tracking data entirely on the edge,[110,124] while applications from Muse and Emotiv can function offline,[125,126] indicating that their core functionality is edge based (Table S4). However, some applications may require more processing power or storage than edge devices can provide or may require centralized for functionality or convenience (e.g., making data available on multiple devices).[127] In such cases, end-to-end encryption should be the default standard for raw data, ensuring users have full control over data access and usage, providing comparable privacy to edge processing.

End-to-End Encryption

For devices where edge processing of raw cognitive biometric data is infeasible or undesirable—due to the need for long-term data storage, processing power, or user preferences to share data for research—end-to-end encryption should be implemented. This means that data are encrypted from captured to use, ensuring only the user or authorized parties can access it.[128] This approach provides strong privacy protections, similar to edge processing, by keeping data inaccessible to unauthorized parties. Additionally, end-to-end encryption alone or in combination with distributed ledger technology[129] maintains data integrity during transmission and storage, preventing tampering and unauthorized modifications. This fosters user trust and enables secure data sharing for legitimate research and development purposes.[130]

While this design framework provides substantial protection against the misuse of raw cognitive biometric data, it is not a complete privacy solution by itself. A company could use edge processing to extract sensitive insights from raw data and then transmit these insights to their servers.[131] A thorough approach to processing cognitive biometric data requires adopting this design framework alongside the broader privacy floor, particularly the informed consent principle, which would prevent the transmission of sensitive insights without consumer's express permission. Implementing these design standards would address most of the privacy concerns discussed earlier, ensuring companies do not access or sell to third parties the personal mental details about the user unrelated to their devices' functions.

Conclusion

Despite robust safeguards provided by existing data protection laws, such as HIPAA in the United States and the GDPR in the European Union, significant gaps remain in protecting cognitive biometric data collected outside of healthcare and clinical settings. These gaps leave individuals' mental privacy vulnerable in an increasingly data-driven world. Expanding legal protections from neural data to the broader category of cognitive biometric data is essential to close these gaps and ensure comprehensive privacy safeguards.

While broadening legal definitions of sensitive data or biometric data to include cognitive biometric data would represent a crucial step forward, it alone cannot fully address the complexities of mental privacy in the digital age. Risks persists, such as the potential for malicious actors to hack user devices,[132] or for companies to violate or modify data use agreements without adequate transparency.[133] Additionally, practices like "tying" products and services to the mandatory sharing of personal data further undermines mental privacy. The proposed UNESCO standards on the ethics of neurotechnology offer a more comprehensive solution,[8] but implementing a privacy floor that strengthens the protections for cognitive biometric data is a necessary foundation.

Striking the right balance between protecting individual interests and fostering innovation remains a significant challenge. In the private sector, data collection is often deemed necessary for innovation and growth.[134] Limiting cognitive biometric data collection might slow innovation in these nascent technologies, impacting both medical and consumer devices, and affect venture capital funding reliant on data generation and sales. Our proposed privacy floor addresses these concerns by allowing data use for product refinement with affirmative consent. This approach empowers consumers to opt into limited data collection and even consent to data transfer voluntarily, potentially even for compensation,[135] fostering a more ethical and transparent relationship between users and companies. This will require companies to demonstrate to users that data sharing is beneficial to both individuals and the collective, empowering them as data co-creators rather than unwilling data subjects.[136]

In the public sector, the vast datasets held by commercial BCI companies, far exceeding those of traditional academic studies, could be used to advance science, medicine, and the public good. Real-world examples, such as the large-scale studies conducted by Apple and Google Fitbit, demonstrate that informed, opt-in consent can support both ethical standards and research and progress, showing that ethical data practices are not only feasible, but also beneficial.[137–139]

Just as the Genetic Information Non-Discrimination Act (GINA) of 2008[140] empowered individuals to share their genetic data without fear of misuse, adopting robust measures to protect cognitive biometric data could similarly empower individuals to secure their mental privacy. By choosing whether, when, and how to share their cognitive biometric data, individuals can contribute to advancements in technology and medicine while maintaining control over their personal information. This balanced approach ensures that innovation and privacy can coexist, leading to a future where both are protected and respected.

ACKNOWLEDGMENTS

This material is based upon work supported by the U.S. National Science Foundation under award No. 2112562. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the U.S. National Science Foundation.

AUTHOR CONTRIBUTIONS

Conceptualization, N.F.; supervision, N.F.; investigation, P.M.; writing – original draft, P.M.; writing – review & editing, M.I., N.F., and P.M.; supplemental tables – P.M.

DECLARATION OF INTERESTS

P.M. received travel reimbursement and hospitality in connection with a one-day ethics workshop conducted by Meta. N.F. and M.I. serve on the UNESCO AHEG Committee. The UNESCO draft referred to in this paper was written collectively by the AHEG Committee, to which both N.F. and M.I. contributed as members of the committee. N.F. serves as an advisor to OpenBCI and is the co-chair of the Neuroethics Working Group of the NIH.

DECLARATION OF GENERATIVE AI AND AI-ASSISTED TECHNOLOGIES

During the preparation of Tables S1 and S2, the authors used Google Translate and ChatGPT to translate and transliterate the content and names of foreign language laws where no suitable translation existed. Google Translate was used to provide the initial translation, and ChatGPT was used for transliteration and in some cases to check the initial translation. The authors reviewed the resulting translations for coherence and consistency and take full responsibility for the content of the publication.

SUPPLEMENTAL INFORMATION

Supplemental information can be found online at https://doi.org/10.1016/j.neuron.2024.09.004.

REFERENCES

1. Farahany, N.A. (2023). The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology (St. Martin's Press).
2. Ienca, M., Haselager, P., and Emanuel, E.J. (2018). Brain leaks and consumer neurotechnology. Nat. Biotechnol. *36*, 805–810. https://doi.org/10.1038/nbt.4240.
3. Ienca, M., and Haselager, P. (2016). Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity. Ethics Inf. Technol. *18*, 117–129. https://doi.org/10.1007/s10676-016-9398-9.
4. Tang, J., LeBel, A., Jain, S., and Huth, A.G. (2023). Semantic reconstruction of continuous language from non-invasive brain recordings. Nat. Neurosci. *26*, 858–866. https://doi.org/10.1038/s41593-023-01304-9.
5. Shen, F.X. (2013). Neuroscience, mental privacy, and the law. Harv. J. Law Public Policy *36*, 653. https://journals.law.harvard.edu/jlpp/wp-content/uploads/sites/90/2013/04/36_2_653_Shen.pdf.
6. Ogonji, M.M., Okeyo, G., and Wafula, J.M. (2020). A survey on privacy and security of Internet of Things. Comput. Sci. Rev. *38*, 100312. https://doi.org/10.1016/j.cosrev.2020.100312.
7. Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108. https://rm.coe.int/1680078b37.
8. UNESCO (2024). Outcome Document of the First Meeting of the AHEG: First Draft of a Recommendation on the Ethics of Neurotechnology (First Version) (Draft at UNESCO). https://unesdoc.unesco.org/ark:/48223/pf0000389768.locale=en.
9. Värbu, K., Muhammad, N., and Muhammad, Y. (2022). Past, Present, and Future of EEG-Based BCI Applications. Sensors *22*, 3331. https://doi.org/10.3390/2Fs22093331.
10. Greenberg, A., Cohen, A., and Grewal, M. (2021). Patent landscape of brain–machine interface technology. Nat. Biotechnol. *39*, 1194–1199. https://doi.org/10.1038/s41587-021-01071-7.
11. Muse (2022). 2022 Muse Brain Health Report. https://choosemuse.com/pages/brain-health-report-2022.
12. Purcher, J. (2023). Apple Invents a next-generation AirPods Sensor System that could measure Biosignals and Electrical Activity of a user's Brain. Patently Apple. https://www.patentlyapple.com/2023/07/apple-invents-a-next-generation-airpods-sensor-system-that-could-measure-biosignals-and-electrical-activity-of-a-users-brain.html.
13. Apple (2023). Biosignal Sensing Device Using Dynamic Selection of Electrodes. Google Patents. https://patents.google.com/patent/US20230225659A1/en.
14. Meta (2021). Inside Facebook Reality Labs: Wrist-based interaction for the next computing platform. Tech at Meta. https://tech.facebook.com/reality-labs/2021/3/inside-facebook-reality-labs-wrist-based-interaction-for-the-next-computing-platform/.
15. Neurotech Reports. The Market for Neurotechnology: 2022-2026. https://www.neurotechreports.com/pages/execsum.html.
16. Smith, M., and Miller, S. (2021). The Future of Biometrics and Liberal Democracy. In Biometric Identification, Law and Ethics, M. Smith and S. Miller, eds. (Springer), pp. 79–95. https://doi.org/10.1007/978-3-030-90256-8_5.
17. Becker, A., and Freitas, C.M.D.S. (2023). Evaluation of XR Applications: A Tertiary Review. ACM Comput. Surv. *56*, 1–35. https://doi.org/10.1145/3626517.
18. Google Fitbit. Stress Management. https://www.fitbit.com/global/us/technology/stress..
19. Tobii. Eye tracking — a catalyst for innovation in AR, VR, and MR. https://www.tobii.com/products/integration/xr-headsets/..
20. Adhanom, I.B., MacNeilage, P., and Folmer, E. (2023). Eye Tracking in Virtual Reality: a Broad Review of Applications and Challenges. Virtual Real. *27*, 1481–1505. https://doi.org/10.1007/s10055-022-00738-z.
21. Meta. Meta Quest. https://www.meta.com/quest.
22. Sony Interactive Entertainment. PlayStation VR. PlayStation. https://www.playstation.com/en-us/ps-vr/..
23. Microsoft. Microsoft HoloLens 2. https://www.microsoft.com/en-us/hololens.
24. Apple. Apple Vision Pro. https://www.apple.com/apple-vision-pro/..
25. ARtillery Intelligence (2023). Extended reality (XR) market size worldwide from 2021 to 2026 (in billion U.S. dollars) [Graph]. Statista. https://www.statista.com/statistics/591181/global-augmented-virtual-reality-market-size/.
26. Google Fitbit. https://www.fitbit.com/global/us/home.
27. Apple. Apple Watch. https://www.apple.com/watch/..
28. Vogels, E. (2020). 21% of Americans Say They Use Smart Watches or Fitness Trackers (Pew Research Center). https://www.pewresearch.org/short-reads/2020/01/09/about-one-in-five-americans-use-a-smart-watch-or-fitness-tracker/.
29. Fortune Business Insights (2024). Fitness Tracker Market Size, Share, & Industry Analysis, By Device Type (Smart Watches, Fitness Bands, Smart Glasses, Smart Clothing, and Others), By Application (Heart Rate Tracking, Sleep Measurement, Glucose Measurement, Sports, Running, and Cycling Tracking), By Distribution Channel (Online, Retail, and Others), and Regional Forecast, 2024-2032. https://www.fortunebusinessinsights.com/fitness-tracker-market-103358.
30. Webster, P. (2024). The future of brain–computer interfaces in medicine. Nat. Med. *30*, 1508–1509. https://doi.org/10.1038/d41591-024-00031-3.

31. Ziogas, A., Mokros, A., Kawohl, W., de Bardeci, M., Olbrich, I., Habermeyer, B., Habermeyer, E., and Olbrich, S. (2023). Deep Learning in the Identification of Electroencephalogram Sources Associated with Sexual Orientation. Neuropsychobiology *82*, 234–245. https://doi.org/10.1159/000530931.

32. Hoppe, S., Loetscher, T., Morey, S.A., and Bulling, A. (2018). Eye Movements During Everyday Behavior Predict Personality Traits. Front. Hum. Neurosci. *12*, 105. https://doi.org/10.3389/fnhum.2018.00105.

33. Liu, Y., Chen, Y., Fraga-González, G., Szpak, V., Laverman, J., Wiers, R.W., and Richard Ridderinkhof, K. (2022). Resting-state EEG, Substance use and Abstinence After Chronic use: A Systematic Review. Clin. EEG Neurosci. *53*, 344–366. https://doi.org/10.1177/15500594221076347.

34. Kröger, J.L., Lutz, O.H.M., and Müller, F. (2020). What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking. In Privacy and Identity Management. Data for Better Living: AI and Privacy, M. Friedewald, M. Önen, E. Lievens, S. Krenn, and S. Fricker, eds. (Springer), pp. 226–241. https://doi.org/10.1007/978-3-030-42504-3_15.

35. Kulasingham, J.P., Vibujithan, V., and De Silva, A.C. (2016). Deep belief networks and stacked autoencoders for the P300 Guilty Knowledge Test. IEEE EMBS Conf. Biomed. Eng. Sci. 127–132. https://doi.org/10.1109/IECBES.2016.7843428.

36. Eckstein, M.K., Guerra-Carrillo, B., Miller Singley, A.T., and Bunge, S.A. (2017). Beyond eye gaze: What else can eyetracking reveal about cognition and cognitive development? Dev. Cogn. Neurosci. *25*, 69–91. https://doi.org/10.1016/j.dcn.2016.11.001.

37. Mason, L., Scrimin, S., Zaccoletti, S., Tornatora, M.C., and Goetz, T. (2018). Webpage reading: Psychophysiological correlates of emotional arousal and regulation predict multiple-text comprehension. Comput. Human Behav. *87*, 317–326. https://doi.org/10.1016/j.chb.2018.05.020.

38. Heller, B. (2020). Watching androids dream of electric sheep: immersive technology, biometric psychography, and the law. Vanderbilt J. Entertain. Technol. Law *23*, 1–52. https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1000&context=jetlaw.

39. Martinovic, I., Davies, D., Frank, M., Perito, D., Ros, T., and Song, D. (2012). On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces. 21st USENIX Secur. Symp. https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final56.pdf.

40. Prochazkova, E., Sjak-Shie, E., Behrens, F., Lindh, D., and Kret, M.E. (2022). Physiological synchrony is associated with attraction in a blind date setting. Nat. Hum. Behav. *6*, 269–278. https://doi.org/10.1038/s41562-021-01197-3.

41. Genser, J., Damianos, S., and Yuste, R. (2024). Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies. Report at Neurorights Foundation. https://neurorightsfoundation.org/reports.

42. Sony Interactive Entertainment (2023). Privacy Policy (PlayStation). https://www.playstation.com/en-us/legal/privacy-policy/.

43. Magic Leap (2023). Magic Leap 2 Devices. https://www.magicleap.com/devices-ml2.

44. Apple (2022). Protecting access to user's health data. https://support.apple.com/guide/security/protecting-access-to-users-health-data-sec88be9900f/web.

45. Apple (2024). Persona & Privacy. https://www.apple.com/legal/privacy/data/en/persona/.

46. Meta (2023). Privacy Policy. https://www.facebook.com/privacy/policy.

47. Emotiv. Data Privacy. https://www.emotiv.com/blogs/glossary/data-privacy..

48. Emotiv (2023). EMOTIV Privacy Policy. https://id.emotivcloud.com/eoidc/privacy/privacy_policy/.

49. Muse (2020). Privacy Policy. https://choosemuse.com/pages/legal#privacy.

50. HTC (2023). Privacy Policy. https://www.htc.com/us/terms/privacy/.

51. Samsung. Samsung Health. Google Play. https://play.google.com/store/apps/datasafety?id=com.sec.android.app.shealth..

52. WHOOP (2024). Full Privacy Policy. https://www.whoop.com/us/en/full-privacy-policy/.

53. Microsoft (2024). Microsoft Privacy Statement. https://privacy.microsoft.com/en-US/privacystatement.

54. California Consumer Privacy Act of 2018, Cal Civ. Code §§ 1798.100-1798.199.100, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (accessed June 13, 2024).

55. Meta (2024). Supplemental Meta Platforms Technologies Privacy Policy. https://www.meta.com/legal/privacy-policy/.

56. Ochang, P., Stahl, B.C., and Eke, D. (2022). The ethical and legal landscape of brain data governance. PLoS One *17*, e0273473. https://doi.org/10.1371/journal.pone.0273473.

57. IAPP (2022). Global Comprehensive Privacy Law Mapping Chart. https://iapp.org/media/pdf/resource_center/global_comprehensive_privacy_law_mapping.pdf.

58. Fazlioglu, M. (2023). IAPP Privacy and Consumer Trust Report – Executive Summary. Report at IAPP. https://iapp.org/media/pdf/resource_center/privacy_and_consumer_trust_report_summary.pdf.

59. FRA (2020). Your rights matter: Data protection and privacy - Fundamental Rights Survey. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-fundamental-rights-survey-data-protection-privacy_en.pdf.

60. Council Regulation 2016/679, 2016 O.J. (L 119) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

61. Solove, D. (2024). Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data. Northwest. Univ. Law Rev. *118*, 1081–1137. https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1555&context=nulr.

62. Tatar, A.B. (2023). Biometric identification system using EEG signals. Neural Comput. Appl. *35*, 1009–1023. https://doi.org/10.1007/s00521-022-07795-0.

63. S.B. 1223, 2023-2024 Leg., Reg. Sess. (Cal. 2024), https://legiscan.com/CA/text/SB1223/id/2962687/California-2023-SB1223-Amended.html.

64. Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1–99, https://www.ilga.gov/legislation/ilcs/ilcs3.Asp?ActID=3004&ChapterID=57 (accessed June 15, 2024).

65. Monroy v. Shutterfly, Inc., Case No. 16 C 10984 (N.D. Ill. 2017), https://casetext.com/case/monroy-v-shutterfly-inc.

66. Spivack, J., Rice, T., and Berrick, D. (2023). Old Laws & New Tech: As Courts Wrestle with Tough Questions Under US Biometric Laws. Immersive Tech Raises New Challenges. https://fpf.org/blog/old-laws-new-tech-as-courts-wrestle-with-tough-questions-under-us-biometric-laws-immersive-tech-raises-new-challenges/.

67. (2022). Theriot V. Louis Vuitton N. Am., 645 F. Supp. 3d 178 (S.D.N.Y). https://casetext.com/case/theriot-v-louis-vuitton-n-am-2.

68. Law No. 21383, Modifica la carta fundamental, para establecer el desarrollo científico y tecnológico al servicio de las personas [Amends the fundamental charter, to establish scientific and technological development at the service of the people], Octubre 25, 2021, Diario Oficial [D.O.], https://www.bcn.cl/leychile/navegar?idNorma=1166983 (translated using Google Translate).

69. McCay, A. (2024). Neurorights: the Chilean constitutional change. AI Soc. *39*, 797–798. https://doi.org/10.1007/s00146-022-01396-0.

70. Asher-Schapiro, A., and Baptista, D. (2023). Hands off my brainwaves: Latin America in race for 'neurorights. Reuters. https://www.reuters.com/article/idUSL8N3AH6D6/.

71. Neurorights Foundation. Neurorights in Chile. https://neurorightsfoundation.org/chile..

72. H.B. 24-1058, 74th Gen. Assemb., 2d Reg. Sess. (Colo. 2024), https://leg.colorado.gov/sites/default/files/2024a_1058_signed.pdf..

73. Moens, J. (2024). Your Brain Waves Are Up for Sale. A New Law Wants to Change That. The New York Times. https://www.nytimes.com/2024/04/17/science/colorado-brain-data-privacy.html.

74. Carlos Henrique Gaguim, *PL n.522/2022*, Câmara dos Deputados (Mar. 9, 2022, 8:02 PM), https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2146384&filename=PL%20522/2022 (translated using Google Translate).

75. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales & Comisión de Protección de Datos Personales, Sistema Nacional de Transparencia, Carta de Derechos de la Persona en el Entorno Digital [Charter on the Rights of the Person in the Digital Environment] (n.d.), https://www.infocdmx.org.mx/doctos/2022/Carta_DDigitales.pdf (accessed June 13, 2024)..

76. The Data Protection Act (2019). Kenya Gazette Supplement No. 181 No. 24. http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf.

77. On Protection of Personal Data, Law of the Republic of Armenia of May 18, 2015 (No. HO-49-N), *translated in* Pashtonakan teghekagir [Official Bulletin], *Law of the Republic of Armenia on Protection of Personal Data*, Arm. Legal Info. Sys., https://www.arlis.am/Annexes/4/Law_Personal_data_protection_EN.pdf..

78. FTC. (2023). Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act. https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf.

79. FTC (2023). FTC Warns About Misuses of Biometric Information and Harm to Consumers. https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers.

80. Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779 (Oct. 19, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0582.

81. Case C-434/16, Peter Nowak v. Data Protection Commissioner, ECLI:EU:C:2017:994 (Dec. 20, 2017), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62016CJ0434..

82. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (2021). COM *206*, (corrigendum) (Apr. 19, 2024). https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf.

83. Farahany, N.A., and Coleman, J.E. (2006). Genetics and Responsibility: To Know the Criminal From the Crime. Law Contemp. Probl *69*, 115–164. https://scholarship.law.duke.edu/lcp/vol69/iss1/7.

84. Farahany, N.A. (2009). Cruel and Unequal Punishments. Wash. Univ. Law Rev. *86*, 859–915. https://scholarship.law.duke.edu/faculty_scholarship/2653.

85. Ienca, M., and Andorno, R. (2017). Towards new human rights in the age of neuroscience and neurotechnology. Life Sci. Soc. Policy *13*, 5. https://doi.org/10.1186/s40504-017-0050-1.

86. H.B. 24-1130, 74th Gen. Assemb., 2d Reg. Sess. (Colo. 2024), https://legiscan.com/CO/bill/HB1130/2024..

87. National Institute of Standards and Technology. Biometrics - Glossary. Computer Security Resource Center. https://csrc.nist.gov/glossary/term/biometrics.

88. Crockford, K. (2022). How to regulate face recognition technology. Nat. Hum. Behav. *6*, 476. https://doi.org/10.1038/s41562-022-01329-3.

89. Yuste, R. (2023). Advocating for neurodata privacy and neurotechnology regulation. Nat. Protoc. *18*, 2869–2875. https://doi.org/10.1038/s41596-023-00873-0.

90. Bar-Zeev, A. (2019). The Eyes Are the Prize: Eye-Tracking Technology Is Advertising's Holy Grail. Vice. https://www.vice.com/en/article/bj9ygv/the-eyes-are-the-prize-eye-tracking-technology-is-advertisings-holy-grail.

91. Spivack, J., and Berrick, D. (2023). Risk Framework for Body-Related Data in Immersive Technologies. Future of Privacy Forum. https://fpf.org/wp-content/uploads/2023/12/FPF-Risk-Framework-for-Body-Related-Data-FINAL-Digital.pdf.

92. McGill, M. (2021). The IEEE Global Initiative on Ethics of Extended Reality (XR) Report–Extended Reality (XR) and the Erosion of Anonymity and Privacy. White paper at IEEE Xplore. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9619999.

93. Allison, B.Z., and Krusienski, D. (2014). Noninvasive Brain-Computer Interfaces. In Encyclopedia of Computational Neuroscience, D. Jaeger and R. Jung, eds. (Springer), pp. 1–13. https://doi.org/10.1007/978-1-4614-7320-6_707-1.

94. Ienca, M., and Malgieri, G. (2022). Mental data protection and the GDPR. J. Law Biosci. *9*, lsac006. https://doi.org/10.1093/jlb/lsac006.

95. UN. https://www.un.org/en/about-us/member-states.

96. DLA Piper. Data Protection Laws of the World. https://www.dlapiperdataprotection.com/index.html..

97. International Association of Privacy Professionals (2024). US State Privacy Legislation Tracker 2024. https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf.

98. Personal Data Protection Act 2012, as amended, https://sso.agc.gov.sg/Act/PDPA2012.

99. Kellmeyer, P. (2021). Big Brain Data: On the Responsible Use of Brain Data from Clinical and Consumer-Directed Neurotechnological Devices. Neuroethics *14*, 83–98. https://doi.org/10.1007/s12152-018-9371-x.

100. Consumer Electronics Association (2015). Guiding Principles on the Privacy and Security of Personal Wellness Data. Future of Privacy Forum. https://fpf.org/wp-content/uploads/2015/10/CEA-Guiding-Principles-on-the-Privacy-and-Security-of-Personal-Wellness-Data-102215.pdf.

101. Budin-Ljøsne, I., Teare, H.J.A., Kaye, J., Beck, S., Bentzen, H.B., Caenazzo, L., Collett, C., D'Abramo, F., Felzmann, H., Finlay, T., et al. (2017). Dynamic Consent: a potential solution to some of the challenges of modern biomedical research. BMC Med. Ethics *18*. https://doi.org/10.1186/s12910-016-0162-9.

102. Org. for Econ. Co-op. and Dev. (2019). Recommendation of the Council on Responsible Innovation in Neurotechnology. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0457.

103. Schaub, F., Balebako, R., and Cranor, L.F. (2017). Designing Effective Privacy Notices and Controls. IEEE Internet Comput. *21*, 70–77. https://doi.org/10.1109/MIC.2017.75.

104. Ienca, M., Fins, J.J., Jox, R.J., Jotterand, F., Voeneky, S., Andorno, R., Ball, T., Castelluccia, C., Chavarriaga, R., Chneiweiss, H., et al. (2022). Towards a Governance Framework for Brain Data. Neuroethics *15*, 20. https://doi.org/10.1007/s12152-022-09498-8.

105. Christovich, M.M. (2015). Why Should We Care What Fitbit Shares?: A Proposed Statutory Solution to Protect Sensitive Personal Fitness Information, UC Law SF Commun. Entertain. J. *38*, 91–116. https://repository.uclawsf.edu/hastings_comm_ent_law_journal/vol38/iss1/4.

106. Zhan, Y., Meng, Y., Zhou, L., and Zhu, H. (2023). Vetting Privacy Policies in VR: A Data Minimization Principle Perspective. IEEE INFOCOM 2023 - IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS). https://doi.org/10.1109/INFOCOMWKSHPS57453.2023.10225937.

107. Information Commissioner's Office. Principle (c): Djujata minimization. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/data-minimisation/..

108. Bonaci, T., Calo, R., and Chizeck, H.J. (2014). App stores for the brain: Privacy & security in Brain-Computer Interfaces. IEEE Int. Symp. Ethics Sci. Technol. Eng. https://doi.org/10.1109/ETHICS.2014.6893415.

109. David-John, B. (2022). Providing Privacy for Eye-Tracking Data with Applications in XR. Dissertation at Georgia Tech Library. https://hdl.handle.net/1853/73252.

110. Apple (2024). Apple Vision Pro Privacy Overview. https://www.apple.com/privacy/docs/Apple_Vision_Pro_Privacy_Overview.pdf.

111. Chizeck, H.J., and Bonaci, T. (2014). Brain-Computer Interface Anonymizer (Google Patents). https://patents.google.com/patent/US20140228701A1/en.

112. Popescu, A.B., Taca, I.A., Nita, C.I., Vizitiu, A., Demeter, R., Suciu, C., and Itu, L.M. (2021). Privacy Preserving Classification of EEG Data Using Machine Learning and Homomorphic Encryption. Appl. Sci. *11*, 7360. https://doi.org/10.3390/app11167360.

113. Xia, K., Duch, W., Sun, Y., Xu, K., Fang, W., Luo, H., Zhang, Y., Sang, D., Xu, X., Wang, F.Y., and Wu, D. (2023). Privacy-Preserving Brain–Computer Interfaces: A Systematic Review. IEEE Trans. Comput. Soc. Syst. *10*, 2312–2324. https://doi.org/10.1109/TCSS.2022.3184818.

114. Yuste, R., Goering, S., Agüerra y Arcas, B., Bi, G., Carmena, J.M., Carter, A., Fins, J.J., Friesen, P., Gallant, J., Huggins, J.E., et al. (2017). Four ethical priorities for neurotechnologies and AI. Nature *551*, 159–163. https://doi.org/10.1038/551159a.

115. Agarwal, A., Dowsley, R., McKinney, N.D., Wu, D., Lin, C.T., De Cock, M., and Nascimento, A.C.A. (2019). Protecting Privacy of Users in Brain-Computer Interface Applications. IEEE Trans. Neural Syst. Rehabil. Eng. *27*, 1546–1555. https://doi.org/10.1109/TNSRE.2019.2926965.

116. David-John, B., Butler, K., and Jain, E. (2023). Privacy-preserving datasets of eye-tracking samples with applications in XR. IEEE Trans. Vis. Comput. Graph. *29*, 2774–2784. https://doi.org/10.1109/TVCG.2023.3247048.

117. Guo, J., Yang, M., and Wan, B. (2021). A Practical Privacy-Preserving Publishing Mechanism Based on Personalized k-Anonymity and Temporal Differential Privacy for Wearable IoT Applications. Symmetry *13*, 1043. https://doi.org/10.3390/sym13061043.

118. Meng, L., Jiang, X., Huang, J., Li, W., Luo, H., and Wu, D. (2023). User Identity Protection in EEG-Based Brain–Computer Interfaces. IEEE Trans. Neural Syst. Rehabil. Eng. *31*, 3576–3586. https://doi.org/10.1109/TNSRE.2023.3310883.

119. Cavoukian, A. Privacy by Design. https://privacy.ucsc.edu/resources/privacy-by-design—foundational-principles.pdf..

120. Shi, W., Cao, J., Zhang, Q., Li, Y., and Xu, L. (2016). Edge Computing: Vision and Challenges. IEEE Internet Things J. *3*, 637–646. https://doi.org/10.1109/JIOT.2016.2579198.

121. Tazrin, T., Rahman, Q.A., Fouda, M.M., and Fadlullah, Z.M. (2021). Li-HEA: Migrating EEG Analytics to Ultra-Edge IoT Devices With Logic-in-Headbands. IEEE Access *9*, 138834–138848. https://doi.org/10.1109/ACCESS.2021.3118971.

122. Shi, W., and Dustdar, S. (2016). The Promise of Edge Computing. Computer *49*, 78–81. https://doi.org/10.1109/MC.2016.145.

123. Shi, W., Pallis, G., and Xu, Z. (2019). Edge Computing [Scanning the Issue]. Proc. IEEE *107*, 1474–1481. https://doi.org/10.1109/JPROC.2019.2928287.

124. Magic Leap (2023, April 16). Magic Leap 2 Eye Tracking Data Transparency Policy. https://www.magicleap.com/eye-tracking.

125. Muse. Using Muse Offline. https://choosemuse.my.site.com/s/article/Using-Muse-Offline?language=en_US..

126. Emotiv. EMOTIV BrainViz. https://www.emotiv.com/products/emotiv-brainviz..

127. Velykoivanenko, L., Niksirat, K.S., Zufferey, N., Humbert, M., Huguenin, K., and Cherubini, M. (2021). Are Those Steps Worth Your Privacy? Fitness-Tracker Users' Perceptions of Privacy and Utility. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. *5*, 1–41. https://doi.org/10.1145/3494960.

128. Backendal, M., Haller, M., and Paterson, K. (2024). End-to-End Encrypted Cloud Storage. IEEE Secur. Priv. *22*, 69–74. https://doi.org/10.1109/MSEC.2024.3352788.

129. Vanin, F.N.d.S., Policarpo, L.M., Righi, R.d.R., Heck, S.M., da Silva, V.F., Goldim, J., and da Costa, C.A. (2022). A Blockchain-Based End-to-End Data Protection Model for Personal Health Records Sharing: A Fully Homomorphic Encryption Approach. Sensors *23*, 14. https://doi.org/10.3390/s23010014.

130. Morey, T., Forbath, T., and Schoop, A. (2015). Customer Data: Designing for Transparency and Trust. Harv. Bus. Rev. https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust.

131. Munn, L. (2020). Staying at the Edge of Privacy: Edge Computing and Impersonal Extraction. Media Commun. *8*, 270–279. https://doi.org/10.17645/mac.v8i2.2761.

132. Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J., and Lv, W. (2019). Edge Computing Security: State of the Art and Challenges. Proc. IEEE *107*, 1608–1631. https://doi.org/10.1109/JPROC.2019.2918437.

133. Confessore, N. (2018). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far (The New York Times). https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

134. Russo, M., Young, D., Feng, T., and Gerard, M. (2021). Sharing Data to Address Our Biggest Societal Challenges (Boston Consulting Group). https://www.bcg.com/publications/2021/data-sharing-will-be-vital-to-societal-changes.

135. Naufel, S., and Klein, E. (2020). Brain-computer interface (BCI) researcher perspectives on neural data ownership and privacy. J. Neural. Eng. *17*, 016039. https://doi.org/10.1088/1741-2552/ab5b7f.

136. Wong, W.H. (2023). We, the Data (MIT Press).

137. Perez, M.V., Mahaffey, K.W., Hedlin, H., Rumsfeld, J.S., Garcia, A., Ferris, T., Balasubramanian, V., Russo, A.M., Rajmane, A., Cheung, L., et al. (2019). Large-Scale Assessment of a Smartwatch to Identify Atrial Fibrillation. N. Engl. J. Med. *381*, 1909–1917. https://doi.org/10.1056/NEJMoa1901183.

138. Stanford Medicine. Apple Heart Study. https://med.stanford.edu/appleheartstudy.html?tab=proxy..

139. Lubitz, S.A., Faranesh, A.Z., Selvaggi, C., Atlas, S.J., McManus, D.D., Singer, D.E., Pagoto, S., McConnell, M.V., Pantelopoulos, A., and Foulkes, A.S. (2022). Detection of Atrial Fibrillation in a Large Population Using Wearable Devices: The Fitbit Heart Study. Circulation *146*, 1415–1424. https://doi.org/10.1161/CIRCULATIONAHA.122.060291.

140. (2008). Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 883. https://www.govinfo.gov/content/pkg/PLAW-110publ233/pdf/PLAW-110publ233.pdf.