# *Neurotechnology In The Workplace: A Futuristic Reality*

Mealey's(R) Data Privacy Report

Online ISSN: 2378-6906 , Print ISSN: 2378-6892

October 2023



**Cite:** 9-6 Mealey's Data Privacy Report 18 (2023)

**Section:** Volume 9, Issue #6

**Length:** 6736 words

## Body

By Jeremy Ben Merkelson, Wendy Kearns, Michael Borgia and Tanner Harris

Imagine a gadget that allows employers to monitor their workers' brainwaves through tiny electrodes hidden inside a keyboard or mouse that sends real-time displays to evaluate emotions, alertness, stress and productivity levels. Not long ago, you'd have thought this concept too farfetched for serious consideration. But advances in neuroscience and artificial intelligence are converging - some say the growth is "on steroids"1 - to provide an affordable and widely available generation of neurotechnology devices that will soon become a pervasive and a regular part of the work landscape. We examine the groundbreaking workplace applications of neurotechnology under development today, including the potential to help detect and aid early intervention efforts to resolve problems of fatigue, burnout, fraud, trade secret misappropriation, and other sanctionable workplace activity, and to boost productivity and worker development. But there are also obvious inherent ethical risks, legal issues, and apprehensions focused on possible irresponsible use of such powerful technologies. Legal risks include those related to biometric data collection, workplace privacy, and perceived or real disability discrimination, among other concerns. As science and technology move into uncharted territory, employers will have to navigate these legal issues for the first time, often with little precedent or guidance.

I. What is Neurotechnology?

Although not yet a frequent topic in legal trade journals, sales of neurotechnology- i.e., technology used to collect, process, and analyze brain or nervous system activity and functionality-are exploding. The science is rapidly advancing.2 The market is growing at a compound annual rate of 12% and is expected to reach $21 billion by 2026.3 Neurotechnology is a unique field because of how closely connected it is to identity, agency, and accountability through human cognition.4 The tech relies on well-established functional neuroimaging techniques, such as fMRI5, EEG6, and fNIRS7, commonly used in medicine and neuroscience research. A key advancement in neurotechnology is Brain-Computer Interfaces, which allow two-way interactions between the brain and machines.8 While some types of advanced neurotechnology already on the market require small surgical procedures to insert implants in the body,9 less invasive technology is also becoming a realistic option for employers.10 So is the application of neuroimaging as a powerful tool for analyzing inner thoughts and perceptions. Coupled with neural decoding methods, raw neurological data can now reveal intentions, visual perceptions, conceptual knowledge, memory, emotions, moods, dreams, beliefs, consciousness, and pain.11 Enhancements in the application of neural

analysis have led to neurotechnology quickly becoming a new way of evaluating mental states with many commercial and managerial applications.

Applications for neurotechnology in employment settings include the use of EEG to monitor fatigue and boost safety. One company sells a fatigue tracking headband, embedded with EEG sensors, that transmits data via Bluetooth to support efficient and cost-effective monitoring of employees while working.12 It can detect an employee becoming dangerously drowsy and sends an early warning alert to both the employee and the manager.13 These are applications that even employees may support, given their ability to promote safety and prevent serious accidents, for example, by alerting long-distance truck drivers when it is time to take a rest break.14

Other applications boost productivity by employing cognitive responses as opposed to physical ones to more efficiently process information. One product's image classification system optimizes complex decision-making by providing a shortcut to the human brain. The software, combined with EEG, can distinguish the characteristic response of a human brain, flagging data without a physical human response. In an application for TSA purposes, for example, an operator sits in front of a computer wearing an EEG headset and watches x-ray images rapidly appear and disappear at a rate of three images per second. The human brain can process visual imagery very quickly, and once the stream ends, the computer screen shows an album of images "flagged" by the operator's brain, such as those that show hidden firearms. The decision-making process to determine whether there's a gun in complex images reportedly takes just 300 milliseconds with no physical action required from the operator.15

The neurotechnology imaging applications may also decode mental states, supporting stress management, work environment responsiveness, and activity monitoring. One company's electric earbuds allow employers to monitor employee mental states, providing insight into employees' levels of focus and stress. Based on this monitoring, employees could be directed to focus on what they are best able to handle at that moment.16 Another company sells a product that produces real-time neurophysiological assessment of employee workloads, with the goal of promoting employment decisions that optimize productivity and employee satisfaction. The sky appears to be virtually limitless in this new frontier, with projected uses that could transform and enhance workplace attentiveness, productivity, and efficiency. But as the technology gets more advanced, the legal risks and ethical concerns get more complicated.

Employers that use these technologies could use them for more than just preventing accidents, addressing fatigue, and helping workers focus on more productive tasks. They also could engage in detailed behavioral monitoring - for example, employers could tell whether an employee whose digital footprints show both work activity and non-work activity occurring simultaneously is actually focused on what they are supposed to be doing at work.17 Of course, employers already use technologies that can monitor employees' activities and productivity, such as software that monitors employees' use of their work devices. But neurotech would take this monitoring in an entirely new direction, providing insights not simply into what employees are doing on a particular device but also into what is going on in employees' heads. Tech that decodes mental states inevitably raises concerns about mindreading or neurotechnological thought apprehension that provides insights into mental states such as memories, emotions, and intentions.18 The question of whether neurotechnology does or will soon enable mindreading is up for debate (depending, of course, on how mindreading is interpreted). Some believe it is a matter of time before neurotechnology enables the interpretation of mental states in real-time. Others believe that due to technological limitations and objections, it is uncertain that these devices will ever achieve actual mindreading capacity.19 Earlier this summer, a study determined that brain scans can translate a person's thoughts into words.20 Mindreading aside, the use of neurotechnology could make available a wealth of information that could be used for a variety of potentially harmful purposes and in ways that raise a hornet's nest of potential legal issues.

## II. Why does it matter?

The use of neurotechnology presents an opportunity for employers to implement a sophisticated and intrusive form of "bossware" to keep tabs on employees,21 but also to take advantage of significant potential for the promotion of health, well-being and economic growth.22 The dystopian potential, however, urges lawful and ethical application of neurotechnology to help and empower employees. If employers are not transparent about what data they are collecting and why, the use of these devices can undermine employee trust and morale, and discourage

employees' adoption even for beneficial purposes. As a proactive measure, organizations should adopt policies and practices that specify how and when neurotechnology may be used and setting reasonable limitations that comply with existing law.

Important privacy issues arise from the collection, storage, use and disclosure of neuroimaging data, as this data may reveal sensitive information about individuals' health and mental life, areas in which people have very clear privacy interests.23 Neurodata may also contain biomarkers for neurological diseases or be used as a means for human authentication. Although data privacy laws do not currently address neurodata expressly, regulators could consider neurodata to be a type of biometric information or other sensitive personal information subject to heightened notice requirements and restrictions on collection, usage, and disclosure. Mental autonomy is a major concern related to neurotechnology. Indeed, skeptics of the technology are right that when people "no longer feel free to 'reflect upon values, decisions, or propositions without threats of consequences,' this may lead to self-censorship and an impaired feeling of autonomy."24 In other words, when people do not feel free to think their own thoughts, freedom of thought, personal autonomy, and authenticity are at risk.25

As the use of neurotechnology expands, so has global recognition of the technology and its associated risks and considerations. International organizations are getting involved. In 2019, the Organisation for Economic Co-operation and Development (OECD) adopted the Recommendation of the Council on Responsibility Innovation in Neurotechnology, the first international standard in this domain.26 The Recommendation calls for responsible innovation in neurotechnology and aims to guide governments and innovators to anticipate and address the ethical, legal, and social challenges of novel neurotechnology, and embodies nine principles, including promoting responsible innovation, safeguarding personal brain data and other information, and anticipating and monitoring potential unintended use and/or misuse.27 The Council of Europe developed a five-year strategic plan for 2020 through 2025 on the ethics of biomedicine, including a chapter on neurotechnology.28 Governments around the world are following suit as Chile and Spain pioneer the protection of neuro-rights.29 Advances in artificial intelligence, as well as the ethical principles around the use of AI can also help neurotechnology advance.30 Actions and investigations by U.S. regulators are already underway for artificial intelligence, and neurotechnology regulation may not be far behind.

1. Privacy and Biometric Data

Compliance with privacy law is probably the first and most serious challenge raised by the use of neurotechnology in the workplace. Of course, common law invasion of privacy claims could be asserted if the technology is used without the employee's authorization.31 At minimum, employers should be transparent with workers about when and how they intend to use these technologies, and give workers a chance to ask questions and exercise any opt-out rights before the technologies are put to use.

Although neuro-rights are not specifically called out by statute in the United States, the use of identifying biometric data is. In 2008, Illinois led the way in biometric legislation with the Biometric Information Privacy Act (BIPA). Among other things, BIPA requires entities that collect or use biometric data to maintain policies and procedures to use this data securely and transparently. Other states, including Texas,32 California,33 *New York,34 North Carolina,35* Florida,36 and Washington37 have since passed their own biometric privacy laws, defining and barring purposes and processes for acquiring, processing, disclosing or selling biometric data.38 Moreover, thirteen US states have enacted so-called "comprehensive" consumer data privacy laws that impose heightened disclosure requirements and usage restrictions on biometrics information and other defined categories of sensitive personal information. While almost all of these laws exempt personal information collected in an employment context, the California Consumer Privacy Act (CCPA) does not.39 Under the CCPA, California employees have a number of rights to control personal information collected about them by their employers, including to access or correct such data, or to have it deleted (subject to various exceptions).40 Biometric privacy laws, particularly BIPA, have stringent enforcement implications for both employers and product developers.*41 In 2019*, the Illinois Supreme Court ruled that a procedural violation of BIPA is sufficient to support a private right of action under BIPA, "giving real teeth to the 200-plus BIPA actions already filed in Illinois."42 Subsequently, the biometric case Rosenbach v. Six Flags, whose litigation path ended in the Illinois Supreme Court, settled for up to $36 million based on allegations that Six Flags failed to comply with BIPA when scanning fingerprints for park entry without consent.43

The threat of potential lawsuits is not the only deterrence from violating BIPA procedural requirements. BIPA violations risk statutory damage awards from $1,000 to $5,000 per violation, damages that could add up significantly and create "ruinous liability" when considering that each individual collection can support a separate violation of BIPA.44 To mitigate risk, companies should evaluate data collected to determine whether BIPA applies, and take appropriate steps to comply with BIPA's substantive and procedural requirements.45 While neuroimaging is not specifically defined as a biometric identifier in existing biometric privacy laws, it is possible that a court could interpret existing statutes to include neuroimaging data as part of the biometric data umbrella.46

Outside the U.S., employees have various rights regarding the collection, use, and storage of personal health and biometric data. Under the European Union's General Data Protection Regulation (GDPR), employees have the right to be informed about what personal data will be collected, how personal data will be used, to access personal data held about them, and to rectify, delete, or block the processing of personal data under certain circumstances.47 In the EU, companies must obtain consumer consent to process personal data, if no other legal basis exists to do so. The rules in the UK are similar in that regard.

There has been discussion of whether to consider "brain data" another type of personal data because it makes people who they are - the core of behavior, emotion, and identity.48 There is a great amount of pressure for neuro-rights governance frameworks to ensure that it is protected from abuse or misuse.49

The UK Information Commissioner's Office (ICO) has issued guidance on the use of neurodata in the workplace, asserting employers must be transparent in the use of neurodata and any use should be fair and lawful.50 ICO guidance recognizes the power imbalance between an employer and employee as "workers are likely to feel that they have no choice but to give [their employer] consent."51 Whether legitimate consent can be freely given in an employment setting is an open question. Germany's legislature, too, has grappled with this consent question in the German Federal Data Protection Act, where the circumstances under which consent was given are considered, including the level of dependence of the employee in the employment relationship, whether legal or economic advantage is achieved for the employee in consenting to the disclosure, or if the employer and employee are pursuing similar interests.52 Employee consent in Germany is freely given only when associated with a legal or economic advantage for the employee or if the employer and employee are pursuing the same interests. GDPR and other laws have similar requirements that consent be "freely given" and cannot be "compelled."53 Guidance from the European Data Protection Board indicates that employees are considered to "consent" to collection of personal data by their employers only in limited circumstances given the "imbalance of power" between employers and their employees.54

Under the GDPR, an entity may only process personal data if it has at least one of six statutorily enumerated lawful basis for doing so. These bases include consent from the individual (although, as noted above, consent may be difficult to obtain, particularly in the employment context), the necessity for the performance of a contract, compliance with a legal obligation, protecting the vital interests of the data subject or of another natural person, necessity for the performance of a task carried out in the public interest, and necessity for the purposes of the business's (or a third party's) legitimate interests, provided that the interests or fundamental rights and freedoms of the individual do not override those legitimate interests.55 Employers must establish that their processing of neurodata is justified under at least one of these bases. Furthermore, employees should have all of their data held centrally in a responsible manner to comply fully with any data requests from employees and ensure data security against unauthorized access. Of course, as with other forms of "new technologies," privacy laws likely would require employers to perform a privacy impact assessment both under European and U.S. laws (i.e., in California).56

2. Discrimination

Employers should be careful to consider the potential algorithmic bias that neurodevices could express and the potential discriminatory uses of neurodata before deploying neurotechnology in the workplace. Using neurodata in the hiring process, for example, could be particularly challenging. It is conceivable that a worker could be subject to discipline, lack of advancement, or other adverse action due to specific mental traits or certain beliefs, or the absence of certain traits that can be determined from neuroimaging.57 Neurotechnology could allow for studying brain activity that indicates the presence or absence of racial bias, an obvious use case for hiring new police

officers.58 Similarly, an employer that uses candidate or employee data showing signs of mental stress could risk disability discrimination claims under federal and state law, if the employer uses such data to make adverse hiring decisions or take other employment actions. Unsurprisingly, such applications could create a significant risk of misidentification and misinterpretation of brain data leading to false attribution of mental traits and states. Moreover, decisions based upon the detection of mental states disregard a person's ability to internally deliberate and mediate those states before translating them into action.

3. Disability Accommodations

Deployment of neurotechnology in the workplace could also have unintended consequences implicating workers' disability rights. For example, data acquired from the use of neurotechnology may suggest that a worker is experiencing fatigue, lack of focus, or other mental conditions that trigger the need to discuss potential reasonable accommodations as part of the interactive dialogue required under the Americans with Disabilities Act. Further, employers must consider what accommodations may and/or must be required to equitably implement the use of neurotechnology. Given these risks, employers rolling out neurotechnology in the workplace should consider whether to adopt policies addressing disability rights implicated by this technology.

4. Workers' Compensation and General Liability Concerns

In addition, employers should remain aware of any liability risks associated with using, or requiring the use of, neurotechnology. For example, the use of this technology may have adverse long-term effects that could trigger workers' compensation liability. There are known concerns with brain stimulation that may cause unsolicited and unpredictable alterations in people's personality, mental traits, and demeanor.59 Employers therefore should consider potential liability associated with biological, psychological, and/or physical injury.

5. Trade Secrets and Reasonable Measures to Protect Data

Neurotechnology also offers a new frontier for employers litigating trade secrets and employee mobility cases. Trade secrets are protected under the federal Defend Trade Secrets Act,60 the U.S. Uniform Trade Secrets Act, as enacted by the various states, and the EU Trade Secrets Directive,61 as well as the Economic Espionage Act,62 which makes it a federal crime in the United States to steal a company's trade secrets. In civil litigation under federal and state law, a trade secret plaintiff must show that it takes "reasonable measures" to protect its trade secret data, typically a fact-specific inquiry based on the level of sensitivity of the data and the employee's level of access.63 With the advent of neurotechnology and its potential for providing an early warning system to employers about the illicit thoughts of employees planning to misappropriate data and leave for a competitor, it may be possible for companies on the hiring end to argue that their new employee's taking of trade secret data is not actionable because the former employer failed to deploy and use neurotechnology that would have given it advance notice to take earlier action to protect their trade secrets. While the reader may now view such an argument farfetched, it is notable that in the early 2000s, most companies did not use digital monitoring technology as they do today, and the use of such monitoring technology is often the core evidence used by trade secret plaintiffs seeking injunctions against their former employees. The standard for what constitutes "reasonable measures" is also constantly evolving in these types of cases and neurotechnology offers a new, even more complex avenue for litigants to argue about what prophylactic steps are necessary to secure trade secret protection.

III. Approaches to Evaluating Use

There are some best practices emerging on the use of neurotechnology. These include the appointment of advisory boards, the development of guidelines, responsible technology transfer, socially responsible investment, and following industry standards and regulatory issues.64 Employers should consider as early as possible who in its organization65 will be best suited to work together to implement these best practices and track changes in the course of conduct regarding this nascent technology.

While it is important for an employer to evaluate its own use of neurotechnology and implement best practices, it also should evaluate the practices of technology providers who are delivering the neurotechnology tools. Common in the technology industry are evaluations of product and service providers' privacy and security practices, industry-

specific regulatory compliance issues, business continuity, adherence to recognized standards, and use of subcontractors. Neurotechnology adds another layer of review that will be required. Some companies may lack the organizational and financial resources to have adequate safeguards when providing this technology. Providers should be evaluated robustly, because the stakes are simply higher for the use of neurotechnology.

Start-up companies developing neurotechnology for the workplace may have the most to offer, but be the least able to proceed cautiously. Because some start-ups, particularly considering available resources and organizational age, will not have the means to tackle these issues all on their own, they must engage in partnerships with others (including their investors) who can.66 Start-ups, who sometimes have intellectual property from university inventors and are less tied to existing corporate norms, can propel innovation in this space and should be viewed as essential to this industry - albeit a set of players that also needs diligence by itself and others.

Companies can learn from others, but there cannot be a one-size-fits-all approach.67 Organizations must consider the purpose of the application, applicable regulatory frameworks, the users, and risk tolerance in determining how it will proceed. Organizations would be well served to prepare now before the time comes to actually use neurotechnology.

IV. Summary

In sum, neurotechnology is sure to put general counsels' offices on their heels. Major unanswered questions include:

* How can consent to the use of this new type of technology be freely given in the employee-employer relationship?

* How does the collection, use, disclosure, and storage of neural data implicate U.S. biometric data laws, consumer privacy laws, and HIPAA?

* Are there hidden algorithmic biases inherent in the use of neurotechnology that employers should be aware of? What are the potential discriminatory uses of this tech?

* What are the risks of biological, psychological, or physical injury from the use of neurotechnology? What level of employee injury, resulting from the use of neurotechnology, could result in claims for workers' compensation?

* How does neural performance tracking implicate disability laws and potentially trigger a duty to offer reasonable accommodations?

* What procedures, tools, and personnel does the employer have to evaluate its own use of neurotechnology? How should it evaluate the provision of neurotechnology by third-party vendors?

While the answers are not clear, organizations should both be excited about the possibilities and tread carefully as we move into this new world. Organizations collecting neurodata should take steps - similar to those recommended for biometric data - to ensure compliance with emerging laws, to address regulatory risks, and avoid private lawsuits. These steps include:

* Assessing whether biometric laws like BIPA and other data privacy laws apply to the collection, use, disclosure, deletion, and storage of neurodata;

* Determining whether possessor and/or protector obligations apply;

* Ensuring compliance with notice and consent requirements;

* Implementing security measures to protect the data;

* Establishing a retention schedule for the data;

* Collecting, using, and disclosing neurodata data only with a permitted statutory basis;68

* Monitoring artificial intelligence advances and their guideposts; and

* Evaluating its technology use and its technology provider carefully.

At minimum, employers should be transparent with workers about when and how they intend to use these technologies, and give workers a chance to ask questions and exercise any opt-out rights before the technologies are put in use. And, if you are thinking it might be wise to seek counsel about what data is retained, and how it is kept and used, to ensure compliance with applicable law and current industry standards: we read your mind.

Endnotes

1. See Olive Cookson, AI driven neurotechnology 'on steroids' needs regulation, says UNESCO, Financial Times (July 12, 2023), *http://ft.com/content/48afd321-5323-449c-aacf-7562f38b2799* (UNESCO intends to build ethical frameworks for neurotechnology and its combination with artificial intelligence (AI)).

2. "The number of neuroscience papers rose from 57,899 in 2011 to 94,456 in 2021, while patents worldwide related to neurotech rose from 418 to 1531 between 2010 and 2020." Id.

3. See Nita A. Farahany. Neurotech at Work, Harv. Bus. Rev., Mar.-Apr. 2023, *https://hbr.org/2023/03/neurotech-at-work*.

4. Hermann Garden et al., Responsible Innovation in Neurotechnology Enterprises 5 (OECD Science, Technology and Industry Working Papers, No. 2019/05), *https://doi.org/10.1787/9685e4fd-en*.

5. Traci Pedersen, All About Functional Magnetic Resonance Imaging (fMRI), PsychCentral, Dec. 13, 2021, *https://psychcentral.com/lib/what-is-functional-magnetic-resonance-imaging-fmri*.

6. Karla Blocka & Daniel Yetman, EEG (Electroencephalogram) Overview, Healthline (Nov. 9, 2021), *https://www.healthline.com/health/eeg*.

7. FNIRS Functional Near Infrared Optical Brain Imaging, BIOPAC Systems, *https://www.biopac.com/application/fnir-functional-near-infrared-optical-brain-imaging/* (last visited Oct. 4, 2023).

8. Frederico Mantellasi, In focus: The challenges of Neurotechnology, Geneva Ctr. for Sec. Pol. (Apr. 11, 2022), *https://www.gcsp.ch/global-insights/focus-challenges-neurotechnology*.

9. Or a more complex one, such as Neuralink's macaque monkey, named Pager, must have undergone for the implant that enabled it to play a video game with its mind. See Isobel Asher Hamilton, Elon Musk's Brain-Chip Company, Neuralink, Released a Video of a Monkey Playing Video Games with its Mind, Insider, April 9, 2021, *https://www.businessinsider.com/elon-musk-neuralink-video-monkey-games-pong-brain-chip-2021-4*.

10. Mantellasi, supra note 8.

11. Timo Istace, Neurorights: The Debate About New Legal Safeguards to Protect the Mind, *37 Issues L. & Med. 95, 97 (2022)*, *https://heinonline.org/HOL/P?h=hein.journals/ilmed37&i=1*.

12. SmartCap, *https://smartcaptech.com* (last visited Oct. 3, 2023), ("LifeBand gathers brain-wave data and processes it through SmartCap's LifeApp, which uses proprietary algorithms to assess wearers' fatigue level on a scale from 1 (hyperalert) to 5 (involuntary sleep).")

13. SmartCap, *https://smartcaptech.com* (last visited Oct. 3, 2023).

14. Julie Weed, Wearable Tech That Tells Drowsy Truckers It's Time to Pull Over, NY Times, Feb 6. 2020, *https://www.nytimes.com/2020/02/06/business/drowsy-driving-truckers.html*.

15. Evan Ackerman & Eliza Strickland, Are You Ready for Workplace Brain Scanning, Nov. 19, 2022, *https://spectrum.ieee.org/neurotech-workplace-innereye-emotiv*.

16. Id.

17. See Farahany, supra note 3.

18. Istace, supra note 11 at 98.

19. Id.

20. Rhiannon Williams, Brain Scans Can Translate a Person's Thoughts into Words, MIT Tech. Rev. (May 1, 2023), *https://www.technologyreview.com/2023/05/01/1072471/brain-scans-can-translate-a-persons-thoughts-into-words/*.

21. Ackerman & Strickland, supra note 15.

22. Garden et al., supra note 4 at 5.

23. Istace, supra note 11 at 102.

24. Id.

25. Id.

26. Recommendation of the Council on Responsible Innovation in Neurotechnology, OECD/LEGAL/0457 (Dec. 12, 2019).

27. Garden et al., supra note 4 at 5.

28. Strategic Action Plan on Human Rights and Technologies in Biomedicine (2020-2025), Council of Eur. (Nov. 19-21, 2019), *https://rm.coe.int/strategic-action-plan-final-e/1680a2c5d2*.

29. Lorena Guzmán H., Chile: Pioneering the Protection of Neurorights, 2022-1 UNESCO Courier 13, *https://en.unesco.org/courier/2022-1/chile-pioneering-protection-neurorightsorg*; see also Avi Asher-Schapiro, 'This is Not Science Fiction,' Say Scientists Pushing for 'Neuro-Rights', Reuters (Dec. 3, 2020), *https://www.reuters.com/article/us-global-tech-rights-idUSKBN28D3HK*.

30. Can AI Principles Make Neurotechnology More Ethical?, ITU News, Oct. 25, 2022, *https://www.itu.int/hub/2022/10/ai-neurotechnology-ethics/*. The sudden advances of generative AI technology and large language models (LLMs) caused a dramatic interest from lawmakers and in self-regulation among AI developers. In July 2023, The Blueprint for an AI Bill of Rights was issued by the White House of the United States and contained eight rules relating to safety, security, and trust, committed to by leading AI developers Amazon, Anthropic, Google., Inflection, Meta, Microsoft, and OpenAI. Neurotechnology could benefit from the lessons and frameworks being worked through by the artificial intelligence community - which, of course, neurotechnology also crosses over with. Of course, neurotechnology is even more complicated.

31. Elements of an Intrusion Claim, Digital Media Law Project, *https://www.dmlp.org/legal-guide/elements-intrusion-claim* (last visited Oct. 3, 2023).

32. Capture or Use of Biometric Identifier Act (CUBI), Tex. Bus. & Com. Code Ann. § 503.001 (barring the capture of biometric identifiers for commercial purposes, unless notice and consent are first given).

33. Cal. Lab. Code Ann. § 1051 (making it a misdemeanor for an employer to require a fingerprint to secure or retain employment and share that information with another employer or third person where it could be used to the detriment of the employee or applicant).

34. N.Y. Lab. Law § 201-a (prohibiting, in some situations, the capture of a fingerprint unless voluntarily given by employee).

35. N.C. Gen. Stat. § 75-61, 65 (requiring entities holding personal information, including biometric data attached to a person's name, to take reasonable measures to protect against unauthorized access).

36. Fla. Stat. § 1002.222(1)(a) (preventing public schools from collecting, obtaining or retaining biometric information of students or immediate family members).

37. My Health My Data Act, 2023 Wash. Sess. Laws Ch. 19, signed into law April 27, 2023 and effective July 23, 2023; Wash. Rev. Code § 19.375.020 (2017) (requiring notice and consent to collect biometric identifiers).

38. Anjali C. Das, Beware of BIPA and Other Biometric Laws - An Overview, Reuters (June 22, 2023), https://www.reuters.com/legal/legalindustry/beware-bipa-other-biometric-laws-an-overview-2023-06-22/ ("While the Illinois BIPA is one of the most widely recognized in the United States, with the threat of sizeable statutory damage awards "per violation," other states have enacted laws governing the collection, storage and use of biometric data," including Texas, California, New York, Colorado, North Carolina, and Florida, with proposed laws similar to BIPA in Arizona, Hawaii, Maryland, Massachusetts, Minnesota, New York, Tennessee, and Vermont).

39. Cal. Civ. Code § 1798.140; CA Prop. 24 (2020), 2020 Cal. Legis. Serv. Prop. 24 Sec. 3(a)(8).

40. Cal. Civ. Code § § 1798.110, 1798.106, 1798.105. Biometric information is "sensitive" personal information under the CCPA and employers must allow employees to limit its use and disclosure, including sale. Id., § § 1798.121, 1798.135.

41. India K. Scarver, Illinois Supreme Court Decides Actual Harm Not Necessary to Sue Under BIPA, The Nat'l L. Rev. (August 8, 2023), https://www.natlawreview.com/article/illinois-supreme-court-decides-actual-harm-not-necessary-to-sue-under-bipa ("the Illinois Supreme Court ruled that a consumer need not demonstrate an adverse effect or specific harm. . . to have standing to sue under. . . Biometric Identity Protection Act (BIPA)").

42. Id.; see also *Rosenbach v. Six Flags, 129 N.E.3d 1197 (Ill. 2019)* (holding that one may be an aggrieved person under BIPA when fingerprint was taken for a season pass without the provision of written consent required by BIPA); see generally *Roberson v. Maestro Consulting Servs., 507 F.Supp.3d 998 (S.D. Ill. 2020)*; see generally *Cothron v. White Castle Sys., 216 N.E.3d 918*, as modified on denial of reh'g (Ill. 2023).

43. *Rosenbach, 129 N.E.3d 1197*; see also Judy Greenwald, Six Flags Settles Illinois Biometric Case, Bus. Ins. (June 16, 2021), https://www.businessinsurance.com/article/20210616/NEWS06/912342570.

44. Scarver, supra note 41; David Rice et al., U.S. District Court Holds That BIPA's Liquidated Damages Are Discretionary, Davis Wright Tremaine (Aug. 15, 2023), https://www.dwt.com/blogs/privacy--security-law-blog/2023/08/illinois-bipa-biometrics-privacy-court-ruling (discussing White Castle Sys.). White Castle faced potential liability of up to $17 billion. Three justices (including the Chief Justice) dissented in White Castle Sys., noting that potentially "punitive, crippling ... ruinous liability" was being imposed on businesses under BIPA and that the decision "will lead to consequences that the legislature could not have intended." *Cothron, 216 N.E.3d 934* (Overstreet, J., dissenting); Subsequently, a federal district judge in Illinois vacated a BIPA damages award of $228 million and set the case for a new jury trial limited to the issue of damages. Rogers v. BNSF Ry., No. 19 C 3082, 2023 WL 4297654, at *13 (N.D. Ill. June 30, 2023); see also David Rice et al., U.S. District Court Holds that BIPA's Liquidated Damages are Discretionary, Davis Wright Tremaine (Aug. 15, 2023), https://www.dwt.com/blogs/privacy--security-law-blog/2023/08/illinois-bipa-biometrics-privacy-court-ruling.

45. Scarver, supra note 40 ("take appropriate steps to comply with the Act's procedural requirements, such as providing written notice of and obtaining written consent to collect, capture, purchase, or otherwise obtain biometric information and setting and publicizing retention parameters and guidelines for permanently destroying biometric identifiers.").

47. Judith Nink, How Will GDPR Affect Employee Data?, GRC World Forums (May 29, 2018), https://www.grcworldforums.com/gdpr/how-will-gdpr-affect-employee-data/21.article.

48. Mantellasi, supra note 9.

49. Id.; Guzmán, supra note 28.

50. See generally Info. Comm'r Off., Employment Practices: Monitoring at Work Draft Guidance at 10 (Oct. 12, 2022), https://ico.org.uk/media/about-the-ico/consultations/4021868/draft-monitoring-at-work-20221011.pdf.

51. Id.

52. See generally Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act] pt. 2, § 26(2) (issued June 30, 2017) (The assessment of the voluntary nature of the consent considers "the dependence of the employee in the employment relationship and the circumstances under which the consent was given. Voluntariness may exist in particular if a legal or economic advantage is achieved. . . or if the employer and the employee pursue similar interests." The employer must nonetheless inform the employee about the purpose of the data processing and employee right of revocation).

53. Guidelines 05/2020 on Consent Under Regulation 2016/679, European Data Protection Board [EDPB] (May 4, 2020).

54. Id.

55. Regulation 2016/679 (General Data Protection Regulation), art. 6, 2018 O.J. (L 127) 1.

56. See Regulation 2016/679 (General Data Protection Regulation), 2018 O.J. (L 127) 1; Cal. Civ. Code § 1798.185(a)(15)(B) (requiring the California Attorney General to issue regulations requiring businesses to perform risk assessments).

57. Istace, supra note 11 at 104.

58. Andrea Lavazza, Thought Apprehension: The "True" Self and the Risks of Mind Reading, 10 AJOB Neurosci. 19, 20 (2019).

59. Istace, supra note 11 at 103.

60. 18 U.S.C. § 1836.

61. Council Directive 2016/943, 2016 O.J. (L 157) 1.

62. 18 U.S.C. § 1833.

63. See, e.g., Solid Wood Cabinet v. Partners Home Supply, No. 13-cv-3598, 2015 U.S. Dist. LEXIS 31655, 2015 WL 1208182 (E.D. Pa. March 13, 2015) (granting summary judgment in favor of defendants finding no evidence of protective steps); Int'l Mezzo Tech. v. Frontline Aerospace, no. 3:10-cv-397, at *18 (M.D. La. Sept. 25, 2014) ("Although [the report at issue] was marked as proprietary and confidential, the plaintiff did not introduce evidence to demonstrate its affirmative efforts to maintain the secrecy of the information contained in the report."); SortiumUSA v. Hunger, No. 3:11-cv-1656-M, 2013 U.S. Dist. LEXIS 191498, 2013 WL 11730655, at *23 (N.D. Tex. March 31, 2013) (granting a motion to dismiss based on plaintiff's failure to mark the information as confidential, require the defendant to execute a confidentiality agreement, and "its failure to plead any other steps to protect the secrecy").

64. Garden, supra note 4 at 6.

65. Id. at 22, 34.

66. Id. at 22.

67. Id.

[Editor's Note: Jeremy Ben Merkelson is a Partner in the Employment Services practice group at Davis Wright Tremaine. Wendy Kearns is the Technology Practice Group Chair and a Partner at Davis Wright Tremaine. Michael Borgia is a Partner in the Privacy & Security practices group at Davis Wright Tremaine. Tanner Harris is a law student at American University and was a Summer Associate at Davis Wright Tremaine in 2022 and 2023. Thanks to Flynn O'Neill, Associate at Davis Wright Tremaine for his assistance with this article. Any commentary or opinions do not reflect the opinions of Davis Wright Tremaine or LexisNexis(r), Mealey Publications(tm). Copyright (c) 2023 by Jeremy Ben Merkelson, Wendy Kearns, Michael Borgia and Tanner Harris. Responses are welcome.]

Do you have news to share? Are you interested in writing a commentary article? Email the Mealey's News Desk at *Mealeys@LexisNexis.com*

**Load Date:** October 27, 2023

---

**End of Document**