SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2025-2026 Regular Session

SB 44 (Umberg)
Version: April 8, 2025
Hearing Date: April 22, 2025
Fiscal: Yes
Urgency: No
CK

SUBJECT

Brain-computer interfaces: neural data

DIGEST

This bill amends the California Consumer Privacy Act of 2018 (CCPA) to require a "covered business" to use neural data collected through a brain-computer interface only for the purpose for which it was collected. This bill requires the covered business to delete the data when the purpose for which it is collected is accomplished.

EXECUTIVE SUMMARY

The CCPA grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. (Civ. Code § 1798.100 et seq.) It places attendant obligations on businesses to respect those rights. The California Privacy Rights Act of 2020 (CPRA) amended the CCPA, limited further amendment, and created a new category of "sensitive personal information" and afforded consumers enhanced rights with respect to that information, including the ability to restrict businesses' use of that information. The emergence of consumer neurotechnologies such as neuromonitoring devices, cognitive training applications, neurostimulation devices, mental health apps, and so called "brain wearables" raised concerns that led to the inclusion of "neural data" within the definition of sensitive information.

This bill takes the next step and regulates "covered businesses," defined as persons that make available a "brain-computer interface." Such entities are required to use neural data collected through these interfaces only for the purpose for which it was collected and to delete such information after that purpose is accomplished.

The bill is sponsored by Oakland Privacy. It is supported by several organizations, including the California Orthopedic Association. No timely opposition was received by the Committee.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Establishes the CCPA, which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. It places attendant obligations on businesses to respect those rights. (Civ. Code § 1798.100 et seq.)

2) Establishes the CPRA, which amends the CCPA. (Civ. Code § 798.100 et seq.; Proposition 24 (2020).)

3) Provides consumers the right to request that a business delete any personal information about the consumer which the business has collected from the consumer. (Civ. Code § 1798.105(a).)

4) Requires a business that collects a consumer's personal information to, at or before the point of collection, inform consumers of the following:
    a) the categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected without providing the consumer with notice consistent with this section;
    b) if the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected without providing the consumer with notice consistent with this section; and
    c) the length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period, provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal

information was collected for longer than is reasonably necessary for that disclosed purpose. (Civ. Code § 1798.100(a).)

5) Grants a consumer the right to request that a business that collects personal information about the consumer disclose to the consumer the following:
    a) the categories of personal information it has collected about that consumer;
    b) the categories of sources from which the personal information is collected;
    c) the business or commercial purpose for collecting, selling, or sharing personal information;
    d) the categories of third parties with whom the business shares personal information; and
    e) the specific pieces of personal information it has collected about that consumer. (Civ. Code § 1798.110.)

6) Provides consumers the right to request that a business that sells or shares the consumer's personal information, or that discloses it for a business purpose, disclose to the consumer specified information, including the categories of personal information collected, shared, sold, and disclosed and the categories of third parties receiving the information. (Civ. Code § 1798.115.)

7) Provides a consumer the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. It requires such a business to provide notice to consumers, as specified, that this information may be sold or shared and that consumers have the right to opt out of the sale or sharing of their personal information. (Civ. Code § 1798.120.)

8) Defines "personal information" as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The CCPA provides a nonexclusive series of categories of information deemed to be personal information, including biometric information, geolocation data, and "sensitive personal information." It does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. (Civ. Code § 1798.140(v).)

9) Extends additional protections to "sensitive personal information," which is defined as personal information that reveals particularly sensitive information such as "neural data," which means information that is generated by measuring the activity of a consumer's central or peripheral nervous system, and that is not inferred from nonneural information. (Civ. Code § 1798.140(ae).)

10) Provides various exemptions from the obligations imposed by the CCPA, including where they would restrict a business' ability to comply with federal, state, or local laws. (Civ. Code § 1798.145.)

11) Permits amendment of the CPRA by a majority vote of each house of the Legislature and the signature of the Governor, provided such amendments are consistent with and further the purpose and intent of this act as set forth therein. (Proposition 24 § 25 (2020).)

This bill:

1) Amends the CCPA to require a covered business to use neural data collected through a brain-computer interface only for the purpose for which the neural data was collected.

2) Requires a covered business to delete neural data collected through a brain-computer interface when the purpose for which the neural data was collected is accomplished.

3) Defines the relevant terms:
    a) "Brain-computer interface" means a system that allows direct communication and control between a person's brain and an external device.
    b) "Covered business" means a person who makes available a brain-computer interface to a person in this state.
4) Includes findings and declaration that the bill furthers the purposes and intent of the CPRA.

COMMENTS

1. California's landmark privacy protection law

As stated, the CCPA grants consumers certain rights with regard to their personal information, as defined. With passage of the CPRA in 2020, the CCPA got an overhaul. Consumers are afforded the right to receive notice from businesses at the point of collection of personal information and the right to access that information at any time. The CCPA also grants a consumer the right to request that a business delete any personal information about the consumer the business has collected from the consumer.

The CCPA provides adult consumers the right, at any time, to direct a business not to sell or share personal information about the consumer to third parties. A business that sells personal information to third parties is required to notify consumers that this information may be sold and that they have the right to opt out of such sales.

The CPRA added a new category of information, sensitive information, which includes data such as precise geolocation and genetic information. Consumers are additionally empowered to limit businesses' use of such information.

2. The emergence of neurotechnologies

Neurotechnologies have been described as the "next technology frontier" by the Institute of Electrical and Electronics Engineers (IEEE), the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.[1] Neurotechnology describes the field of science and engineering in which the nervous system is interfaced with technical devices, using neural interfaces to read or write information into the central nervous system (CNS), the peripheral nervous system (PNS), or the autonomic nervous system (ANS). There are a number of methods to do this, both invasive and noninvasive.

Like with most advanced technologies, there are tremendous possibilities:

> Neurotechnologies can provide insights into brain or nervous system activity, or can influence brain or nervous system function. Essentially, neurotechnologies have the potential to help neuroscientists gather information that might help uncover some of the secrets of the biology underlying the normal and pathological functioning of the human brain – arguably the most complex and least understood organ of the human body – as well as delivering practical therapeutic or rehabilitative solutions in the clinical care of neurological disorders to help ease the personal and socioeconomic burden of these conditions. Adopting a technology-based approach can also have benefits for research, allowing the use of more sensitive endpoints that will accelerate data gathering and evidence generation in clinical trials.[2]

The infinite applications are also being explored for consumer products: "Eventually, neurotechnologies could enable commercial devices, like phones, powered by mind control. Neurotechnologies could also potentially enable features like a thought-to-text writing function, or virtual and augmented reality devices assisted by brain control for purposes of entertainment."[3] For example, a few years back, Facebook purchased a neurotechnology startup, as part of efforts to develop a wristband for controlling

---

[1] *Neurotechnologies: The Next Technology Frontier*, IEEE Brain, https://brain.ieee.org/topics/neurotechnologies-the-next-technology-frontier/. All internet citations are current as of April 2, 2025.
[2] Roongroj Bhidayasiri, *The grand challenge at the frontiers of neurotechnology and its emerging clinical applications* (January 17, 2024) Front Neurol, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10827995/pdf/fneur-15-1314477.pdf.
[3] *See* fn. 1.

smartphones, computers and other digital devices without having to touch a screen or keyboard.[4]

With the emergence of these consumer neurotechnology devices comes not only concern that regulatory oversight is insufficient to, for example, assess efficacy claims, many are sounding alarms around the privacy implications:

> A last bastion of privacy, our brains have remained inviolate, even as sensors now record our heartbeats, breaths, steps and sleep. All that is about to change. An avalanche of brain-tracking devices—earbuds, headphones, headbands, watches and even wearable tattoos—will soon enter the market, promising to transform our lives. And threatening to breach the refuge of our minds.
>
> Tech titans Meta, Snap, Microsoft and Apple are already investing heavily in brain wearables. They aim to embed brain sensors into smart watches, earbuds, headsets and sleep aids. Integrating them into our everyday lives could revolutionize health care, enabling early diagnosis and personalized treatment of conditions such as depression, epilepsy and even cognitive decline. Brain sensors could improve our ability to meditate, focus and even communicate with a seamless technological telepathy—using the power of thoughts and emotion to drive our interaction with augmented reality (AR) and virtual reality (VR) headsets, or even type on virtual keyboards with our minds.
>
> But brain wearables also pose very real risks to mental privacy, freedom of thought and self-determination. As these devices proliferate, they will generate vast amounts of neural data, creating an intimate window into our brain states, emotions and even memories. We need the individual power to shutter this new view into our inner selves.
>
> Employers already seek out such data, tracking worker fatigue levels and offering brain wellness programs to mitigate stress, via platforms that give them unprecedented access to employees' brains. Cognitive and emotional testing based on neuroscience is becoming a new job screening norm, revealing personality aspects that may have little to do with a job. In China, train conductors of the Beijing-Shanghai line, the busiest of its kind in the world, wear brain sensors throughout their work day. There are even reports of Chinese employees being sent home if their brain activity shows less than stellar brain metrics. As companies embrace brain

[4] Queenie Wong & Scott Stein, *Facebook buys startup working on technology that lets you control computers with your mind* (September 23, 2019) CNET, https://www.cnet.com/science/facebook-buys-ctrl-labs-to-work-on-a-wristband-that-will-let-you-control-computers-with-your-mind/.

> wearables that can track employees' attention, focus and even boredom, without safeguards in place, they could trample on employee's mental privacy, eroding trust and well-being along with the dignity of work itself.[5]

The Future of Privacy Forum provides some privacy and ethical considerations for the emerging technology it refers to as "brain-computer interfaces" (BCI), which it defines as computer-based systems that directly record, process, analyze, or modulate human brain activity in the form of neurodata that is then translated into an output command from human to machine:

> Some BCI implementations raise few, if any, privacy issues. For example, individuals using BCIs to control computer cursors might not not reveal any more personal information than typical mouse users, provided BCI systems promptly discard cursor data. However, some uses of BCI technologies raise important questions about how laws, policies, and technical controls can safeguard inferences about individuals' brain functions, intents, or emotional states. These questions are increasingly salient in light of the expanded use of BCIs in:
>
> - **Health and Wellness** – where BCIs monitor fatigue, diagnose medical conditions, stimulate or modulate brain activity, and control prosthetics and devices like wheelchairs.
> - **Gaming** – where BCIs augment existing gaming platforms and offer players new ways to play using devices that record and interpret their neural signals.
> - **Employment** – where BCIs monitor workers' engagement to improve safety during high-risk tasks, alert workers or supervisors of dangerous situations, modulate workers' brain activity to improve performance, and provide tools to more efficiently complete tasks.
> - **Education** – where BCIs can track student attention, identify students' unique needs, and alert teachers and parents of student learning progress.
> - **Smart Cities** – where BCIs could provide new avenues of communication for construction teams and safety workers and enable potential new methods for connected vehicle control.
> - **Neuromarketing** – where marketers incorporate the use of BCIs to intuit consumers' moods, and to gauge product and service interest.

---

[5] Nita Farahany, *Wearable Brain Devices Will Challenge Our Mental Privacy* (March 27, 2023) Scientific American, https://www.scientificamerican.com/article/wearable-brain-devices-will-challenge-our-mental-privacy/.

- **Military** – where governments are researching the potential of BCIs to help rehabilitate soldiers' injuries and enhance communication.

It is important for stakeholders in this space to delineate between the current and near future uses and the far-distant notions depicted by science fiction creators. The realistic view of capabilities is necessary to credibly identify urgent concerns and prioritize meaningful policy initiatives. While the potential uses of BCIs are numerous, BCIs cannot at present or in the near future "read a person's complete thoughts," serve as an accurate lie detector, or pump information directly into the brain.

As BCIs evolve and are more commercially available across numerous sectors, it is paramount to understand the real risks such technologies pose. BCIs raise many of the same risks posed by home assistants, medical devices, and wearables, but implicate new and heightened risks associated with privacy of thought, resulting from recording, using, and sharing a variety of neural signals. Risks include, but are not limited to:

- Collecting, and potentially sharing, sensitive information related to individuals' private emotions, psychology, or intent;
- Combining neurodata with other personal information to build increasingly granular and sensitive profiles about users for invasive or exploitative uses, including behavioural advertising;
- Making decisions that significantly impact patients, employees, or students based on information drawn from neurodata (with potential but distinct risks if the conclusions are accurately, or inaccurately drawn);
- Security breaches compromising patient health and individual safety and privacy;
- A lack of meaningful transparency and personal control over individuals' neurodata; and
- Surveilling individuals based on the collection of sensitive neurodata, especially from historically and heavily surveilled communities.[6]

3. Protecting our neural data

Responding to the privacy concerns raised by these neurotechnologies, SB 1223 (Becker, Ch. 887, Stats. 2024) included "neural data" into the definition of sensitive personal information for purposes of the CCPA. Neural data is defined as information that is

[6] Jeremy Greenberg, *Brain-Computer Interfaces: Privacy and Ethical Considerations for the Connected Mind* (September 21, 2021) Future of Privacy Forum, https://fpf.org/blog/brain-computer-interfaces-privacy-and-ethical-considerations-for-the-connected-mind/?utm_source=chatgpt.com.

generated by the measurement of the activity of an individual's CNS or PNS, and that is not inferred from nonneural information.

This bill takes the next step by regulating "covered businesses," persons that make available BCIs to a person in this state. It defines BCI to mean a system that allows direct communication and control between a person's brain and an external device.

The bill amends the CCPA to limit a covered business' use of neural data collected through a BCI to the purpose for which the neural data was collected. To protect the security of this information and the privacy of the individual, the covered business is required to automatically delete this neural data when the purpose for which it was collected is accomplished.

According to the author:

> SB 44 is a critical step in the right direction to ensure that we are protecting a person's most sensitive information. The advancement of Brain-Computer Interface (BCI) technology into mainstream society represents both an exciting and challenging set of circumstances for scientists, researchers, and lawmakers alike. BCIs allow direct communication between a person's brain and external devices. Originally, these were created for medical purposes like helping to improve cognitive function and restoring mobility for paralyzed patients. In recent years, however, BCIs have attracted additional interest from technology companies for expanded capabilities with the most notable example being Elon Musk's Neuralink and discussion about the technology being used for gaming, workplace efficiency, entertainment, and other possibilities.
>
> Brain data collected by BCIs has the potential to reveal sensitive personal details about a person's thoughts, emotions, cognitive processes, and even subconscious thoughts. In the wrong hands, the consequences of misused or unprotected neural data could be severe. Protecting this highly sensitive information from unauthorized access or misuse is a crucial piece of both medical and consumer data protection privacy. At the most extreme, nobody deserves their innermost thoughts and feelings being perverted or manipulated by the likes of Elon Musk. SB 44 will ensure user protection by mandating that a covered provider shall only use the neural data for the purpose in which it was stated to be collected for. Lastly, it would require the covered provider to delete the data when the purpose for which it was collected is completed.

Writing in support, Oakland Privacy, the sponsor of the bill, states:

> This bill, SB 44, ensures that all persons or entities that make available a brain-computer interface in the state, whether or not they are large enough to be a covered business under the rest of the CPRA, are subject to enhanced data minimization and data deletion requirements for the neural data they collect.
>
> This is important for a number of reasons. As a start-up industry and a fairly new technological innovation, it is certainly possible that an entity may be utilizing this brain-computer interface technology in such a limited or trial fashion that they may not meet the definition of a covered business under the CPRA for some period of time that they are collecting neural data.
>
> That can leave some neural data, and more importantly, the people from whom the neural data was collected, in a regulatory no-mans-land when a start-up company too small for CPRA oversight would have the freedom to use, share, sell and retain the neural data they collect freely. SB 44 plugs this gap, in recognition that the capacity of neural data for the prediction, influence, manipulation and alteration of human behavior is extremely powerful, and potentially dangerous in the wrong hands.
>
> The California Privacy Rights Act provides significant protections for the sensitive personal data that it covers. Consumers have the right to opt out of the sale or share of their sensitive personal information, and additionally can restrict its uses to only the purpose for which it was collected and request that it be deleted. However, and this is important, the consumer must specifically request in a verifiable form for that these data minimization and data deletion provisions be executed.
>
> The Legislature decided in the 2018 enactment of the California Consumer Privacy Act (CCPA) to use the optout standard as the baseline for privacy rights, and in 2020, with the adoption of CPRA (Proposition 24), voters enacted data minimization at the request of the consumer for information defined as highly sensitive. And as mentioned, in 2024, SB 1223 explicitly added neural data to the categories of information defined in CPRA as highly sensitive.
>
> Senate Bill 44 posits that the use and retention of neural data is so critical that it cannot be left to the discretion of the individual consumer to limit.

4. Furthering the purpose and intent of the CPRA

Section 25 of the CPRA requires any amendments thereto to be "consistent with and further the purpose and intent of this act as set forth in Section 3." Section 3 declares that "it is the purpose and intent of the people of the State of California to further protect consumers' rights, including the constitutional right of privacy." It then lays out a series of guiding principles. These include various consumer rights such as:

- consumers should know who is collecting their personal information;
- consumers should have control over how their personal information is used; and
- consumers should benefit from businesses' use of their personal information.

Section 3 also includes a series of responsibilities that businesses should have. These include:

- businesses should specifically and clearly inform consumers about how they use personal information; and
- businesses should only collect consumers' personal information for specific, explicit, and legitimate disclosed purposes.

Section 3 also lays out various guiding principles about how the law should be implemented.

This bill provides stronger protections for this incredibly sensitive information. This allows for a fuller realization of the benefits intended by the law. Therefore, as it explicitly states, this bill "furthers the purposes and intent of the California Privacy Rights Act of 2020."

SUPPORT

Oakland Privacy (sponsor)
California Orthopedic Association
Consumer Federation of California
Science Corporation

OPPOSITION

None known

RELATED LEGISLATION

Pending Legislation:

SB 7 (McNerney, 2025) prohibits, among other things, an employer from using an automated decision system that obtains a worker's neural data. SB 7 is currently in this Committee.

AB 1221 (Bryan, 2025) prohibits, among other things, an employer from using a workplace surveillance tool that obtains an employee's neural data. AB 1221 is currently in the Assembly Privacy and Consumer Protection Committee.

Prior Legislation: SB 1223 (Becker, Ch. 887, Stats. 2024) *See* Comment 3.

****