Date of Hearing: July 1, 2026
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 1130 (Reyes) – As Amended June 25, 2026

SENATE VOTE: 30-8

SUBJECT: Invasion of privacy: wearable recording devices

SYNOPSIS

Rapid advancements in wearable technology have exposed significant gaps in existing privacy protections. Devices such as AI-enabled smart glasses – including products like Ray-Ban Meta Smart Glasses and other emerging wearable technologies – closely resemble ordinary eyewear while containing cameras, microphones, and artificial intelligence systems capable of recording audio, capturing video, and processing information in real time. Because these devices are discreet and increasingly normalized in everyday settings, individuals may be recorded, analyzed, or surveilled without their knowledge or consent.

Intrusive encounters with people using wearable surveillance devices are becoming more common. According to a March 2026 article in Wired *magazine, popular influencer accounts with millions of followers are simply men wearing Meta Ray-Ban glasses who are "prowling sun-soaked beaches and corridors of city nightlife so they can showcase their attempts to pick up women."*

This bill places limits on a person operating a wearable recording device and prohibits the manufacture and sale of devices designed to thwart the light or sound on the device that alerts someone that they are being recorded.

This bill enjoys the support of Oakland Privacy, Consumer Reports, the California Federation of Labor Unions, and California Civil Liberties Advocacy. It is opposed by the California Chamber of Commerce, the California Restaurant Association, the Computer and Communications Industry Association, and TechNet.

This bill was previously heard by the Public Safety Committee, where it passed on a 7-2 vote.

EXISTING LAW:

1) Provides, pursuant to the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const., art. I, § 1.)

2) Permits a person to bring an action in tort for an invasion of privacy and provides that in order to state a claim for violation of the constitutional right to privacy, a plaintiff must establish the following three elements: (1) a legally-protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by the defendant that constitutes a serious invasion of privacy. (*Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal.4th 1, 40.)

3) Renders an individual liable for constructive invasion of privacy when that individual attempts to capture, in a manner that is offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of another engaging in a private, personal, or familial activity, through the use of any device, regardless of whether there is a physical trespass, if this image, sound recording, or other physical impression could not have been achieved without a trespass unless the device was used. (Civ. Code § 1708.8.)

4) Prohibits a person or entity from compelling a manufacturer or other entity providing the operation of a voice recognition feature to build specific features for the purpose of allowing an investigative or law enforcement officer to monitor communications through that feature. (Bus. & Prof. Code § 22948.20(d).)

5) Makes it a misdemeanor for a person to use a concealed camcorder, motion picture camera, or photographic camera of any type, to secretly videotape, film, photograph, or record by electronic means, another identifiable person who may be in a state of full or partial undress, for the purpose of viewing the body of, or the undergarments worn by, that other person, without the consent or knowledge of that other person, in the interior of a bedroom, bathroom, changing room, fitting room, dressing room, or tanning booth, or the interior of any other area in which that other person has a reasonable expectation of privacy, with the intent to invade the privacy of that other person. (Pen. Code, § 647 (j)(3)(A).)

6) Defines "identifiable" as "capable of identification, or capable of being recognized, meaning that someone, including the victim, could identify or recognize the victim." Specifies that the victim's identity is not required to actually be established. (*Ibid*.)

7) Makes it a crime to intentionally and without the consent of all parties eavesdrop or record a confidential communication. (Pen. Code, § 632 (a).)

8) Defines "confidential communication" as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made in a public gathering or in any legislative, judicial, executive or administrative proceeding open to the public, or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded." (Pen. Code, § 632 (c).)

9) Provides a right for people injured by a violation of specified provisions, in which the plaintiff may obtain the greater of $5,000 per violation or three times actual damages, as well as injunctive relief. (Pen. Code, § 631 (a).)

THIS BILL:

1) Prohibits a person or entity from manufacturing, selling, delivering, holding, or offering for sale in commerce in this state either of the following:

    a. A wearable recording device without a light, sound, or other indicator that is prominent enough that a reasonable person in the vicinity would be aware that the device is recording.

b. Any technology that is designed for the purpose of, marketed for, or likely primarily used for enabling a person to disable any light or other device on a wearable recording device that indicates that the device is capturing sound or video.

2) Prohibits a person from purchasing, trading for, or otherwise acquiring any technology described in (1)(b) above.

3) Prohibits a person from using any technology to permanently or temporarily disable any light or other device on a wearable recording device that indicates that the device is capturing sound or video if the device would otherwise indicate that it is capturing sound or video.

4) Makes a violation of (1), (2), or (3) punishable by a civil penalty with a fine of $2,500 per violation.

5) States, for the purpose of the civil violation, "wearable recording device" has the same meaning as it does in the Penal Code.

6) Makes it a misdemeanor, punishable by imprisonment of up to one year and a fine of up to $1,500, for a person to do either of the following:

a. Disable any light sound or other indicator on a wearable recording device that indicates that the device is capturing sound or video.

b. Operate a wearable recording device to capture sound or video of any other person in any area within a place of business where the person has a reasonable expectation of privacy unless the person operating the device has the explicit consent of that person to capture sound or video of that person.

7) Provides that the fact that a person takes a photograph or makes an audio or video recording of a public officer or peace officer, while the officer is in a public place or the person taking the photograph or making the recording is in a place the person has the right to be does not constitute in and of itself a violation of these provisions nor does it constitute reasonable suspicion to detain the person or probable cause to arrest the person.

8) States that it does not apply to the use of hearing aids, augmentative and alternative communication devices, and similar devices by a person afflicted with impaired hearing or any communication disorder when the hearing device is used for the purpose of overcoming impairment or disorder to permit the hearing of sounds ordinarily audible to the human ear or to support communication with the person.

9) Adds the crime created in this bill to the statutes that exempt specified individuals from the wiretapping, eavesdropping, and unlawful recording statutes.

10) Adds the crime created in the bill to the existing criminal statutes prohibiting wiretapping, eavesdropping, and unlawful recording for purposes of enhancement penalties when there are prior convictions for these crimes.

11) Defines the following:

a. "Place of business" means "any physical office or retail establishment in which members of the public receive goods or services from the business."

b. "Wearable recording device" means "any device that is designed to be worn on or attached to the body that has the capacity to make sound or video recordings or transmit data received by the device to another device or to the internet.."

12) Provides that a wearable recording device does include a body-worn camera when used by a public officer or peace officer in the course of their official duties.

COMMENTS:

1) **Author's statement**. According to the author:

> Artificial intelligence and wearable technology are transforming the way we communicate and interact with the world. Devices such as smart glasses and other body-worn recording devices are becoming more common in everyday life. While innovation should be welcomed, it must not come at the expense of Californians' fundamental right to privacy.
>
> California has long been a national leader in privacy protections. However, many of our existing eavesdropping and recording statutes were written with traditional technologies in mind, telephones, handheld cameras, and tape recorders. Wearable devices present new challenges. They are often designed to look like ordinary eyewear or fashion accessories, making it difficult, if not impossible, for bystanders to know or consent when they are being recorded. In some cases, recording indicator lights can be subtle, disabled, or modified, increasing the risk of covert surveillance.
>
> SB 1130 modernizes California law to address these emerging concerns. The bill defines wearable recording devices and prohibits recording in areas within places of business where individuals have a reasonable expectation of privacy, unless explicit consent is provided. It also prohibits tampering with or disabling recording indicators and restricts the manufacture, sale, purchase, or use of technology intended to conceal recording activity.
>
> This measure does not prohibit innovation, nor does it prevent lawful recording. Instead, it reinforces core principles of transparency, consent, and accountability. As technology evolves, our laws must evolve with it to ensure that privacy protections remain meaningful.
>
> SB 1130 provides clear standards for businesses, consumers, and law enforcement, while protecting Californians' dignity and reasonable expectations of privacy.

2) **Privacy in public places.** A major problem with US privacy laws, including California's, is its continued embrace of the belief "that anything exposed to the public, or data available to the public, or even information shared with others lacks any privacy interest because it is not totally secret. This flawed understanding of privacy creates two common and severe limitations of privacy law—a failure to protect privacy in public or publicly-available data."[1] A commonly repeated belief is that people in public should have no expectation of privacy. As it pertains to this bill, including being recorded by wearable surveillance technology. This secrecy paradigm misses the foundational importance of obscurity as a privacy protection.[2]

---

[1] Solove, Daniel J. *Privacy in Authoritarian Times: Surveillance Capitalism and Government Surveillance*, George Washington University Law School (Jan. 19, 2025). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5103271.
[2] *Ibid.*

As Professor Daniel Solove notes:

> Most people do not live like hermits; they engage in their life's activities in places where other people congregate. People expect that their activities are private because they are obscure – others won't be paying attention or watching or listening. Modern surveillance technologies, including wearable surveillance technology, have eroded this sense of obscurity. Conversations can be easily recorded, and movements meticulously tracked. As individuals use digital technologies, they leave behind a trail of personal data that previously was forgotten or never collected. [3]

The principle of obscurity emphasizes that just because someone is in a public place, that does not mean privacy is forfeited. Although their movements in public may not be secret, obscurity imposes significant limits on accessibility.[4]

As discussed in the Senate Privacy, Digital Technologies, and Consumer Protection Committee analysis, compounding the loss of obscurity is using devices to furtively record people:

> Inherently, wearable devices that are able to capture images and video raise concerns about surreptitious recording. The potential privacy concerns are highlighted by a reported case involving an influencer who realized the person providing her waxing services was wearing Meta glasses during the wax. This is why manufacturers like Meta have been incorporating small LED lights or similar signals to alert bystanders that a device is actively recording, a modest but meaningful concession to privacy concerns. However, when someone physically obscures, disables, or modifies that indicator, they are not simply bending a technical rule; they are making a conscious, premeditated choice to deceive the people around them. A simple search online reveals the various products that are being actively offered for sale that allow for this obstruction, from dark stickers to place over the light indicators to hardware modifications that bypass the indicator function.

According to reports, intrusive encounters with people using wearable devices are becoming more common. According to a March 2026 article in *Wired* magazine, popular influencer accounts with millions of followers are simply men wearing Meta Ray-Ban glasses who are "prowling sun-soaked beaches and corridors of city nightlife so they can showcase their attempts to pick up women."[5]

3) **Need for this bill.** The author provides the following context for this bill:

> Rapid advancements in wearable technology have exposed significant gaps in existing privacy protections. Devices such as AI-enabled smart glasses- including products like Ray-Ban Meta Smart Glasses and other emerging wearable technologies - closely resemble ordinary eyewear while containing cameras, microphones, and artificial intelligence systems capable of recording audio, capturing video, and processing information in real time. Because these devices are discreet and increasingly normalized in everyday settings, individuals may be recorded, analyzed, or surveilled without their knowledge or consent.

---

[3] *Ibid.*
[4] Solove (2025)
[5] Miles Klee, "The Rise of the Ray-Ban Meta Creep," *Wired* (Mar. 23, 2026) https://www.wired.com/story/the-rise-of-the-ray-ban-meta-creep/.

California's existing privacy laws were largely written before the emergence of wearable recording technology integrated into everyday accessories. While statutes addressing eavesdropping, recording, and expectations of privacy prohibit certain forms of non-consensual recording, they do not fully account for devices that can continuously capture and process information in a passive or unobtrusive manner. In many cases, current law relies on clear notice that recording is occurring or assumes that recording devices are visible and identifiable. Wearable technologies challenge those assumptions by embedding recording capabilities into commonplace objects that appear indistinguishable from ordinary consumer products.

For example, some wearable devices rely on small indicator lights or subtle visual cues to signal recording. However, these indicators can be difficult to notice in real-world settings and may not provide meaningful notice to individuals nearby. As a result, people may unknowingly have their conversations, images, or activities recorded and stored without an opportunity to consent or object. Existing statutes also do not adequately address situations where recording indicators are disabled, obscured, or tampered with, further undermining transparency.

Additionally, current law provides limited guidance on how to regulate devices that combine recording capabilities with artificial intelligence tools capable of analyzing or storing captured information. These technologies can transform ordinary interactions - such as conversations in public spaces or interactions in businesses- into permanent digital records that may be uploaded, processed, or shared without the knowledge of those being recorded.

This gap is particularly concerning for individuals who may already face heightened risks of harassment, stalking, or surveillance, including women, children, and other vulnerable communities. Without clearer rules governing wearable recording devices, individuals have little visibility or control over when their personal information is being captured or how it may be used.

As wearable technologies continue to evolve and become more widespread, California law must be updated to ensure that privacy protections keep pace with technological innovation. Clarifying standards for consent, transparency, and the responsible use of wearable recording devices is necessary to preserve individuals' reasonable expectations of privacy in an increasingly connected world.

4) **What this bill would do.** This bill seeks to shut down the market for technology to disable the only clear signal to bystanders that a pair of sunglasses or another wearable device is actively spying on them. It prohibits manufacturing and selling any technology in this state that enables a person to disable any light or other device on a wearable recording device that indicates that the device is capturing sound or video.

In addition, at the request of the Committee, the author has amended the bill to include prohibiting the manufacturing of wearable devices that do not include an indicator that the device is recording.

On the consumer side, the bill prohibits the purchase or acquisition of such technology and the use of it to disable these indicators and imposes criminal penalties for disabling indicators or for operating a wearable recording device to capture sound or video of any other person without their consent in any area within a place of business where the person has a reasonable expectation of privacy.

Additionally, the bill is enforceable under existing law, which provides an action for persons injured by a violation of the California Invasion of Privacy Act. In such an action, the plaintiff may obtain the greater of $5,000 per violation or three times actual damages, as well as injunctive relief.

ARGUMENTS IN SUPPORT: Consumer Reports writes in support:

> Today, Californians' fundamental right to privacy is under threat by the growing proliferation of wearable recording technologies. These devices, while undoubtedly technically impressive, can facilitate the frictionless and surreptitious recording of individuals, eroding well-established norms of personal agency and informed consent. Perhaps the best-known product in the wearable category is Meta's AI-enabled smart glasses, produced in partnership with eyewear maker EssilorLuxottica and licensed to brands such as RayBan and Oakley. Meta reportedly sold several million smart-glass units in 2025 and are reportedly seeking to produce 20-30 million units by the end of 2026.
>
> Very quickly, these devices have generated a series of frightening incidents. Just last month, it was revealed that Meta was sending raw video collected from glasses to its Kenya-based contractors for the purpose of training and labeling for its AI systems. This practice resulted in video of consumers' bathroom visits, sexual activities, and other intimate moments being watched by human reviewers. A recent BBC investigation surfaced numerous examples of women being secretly recorded by men in public places with the resulting videos going viral and resulting in embarrassment, unwanted attention, and online harassment. And in another recent story, a woman realized mid-appointment that her Brazilian wax technician was wearing Meta glasses — and though the technician assured her the glasses were not recording, the woman had no way of verifying that this was the case.
>
> This last example is exactly what SB 1130 seeks to address. Under the bill, an individual would need to obtain explicit consent before recording a person in "any area within a place of business where the person has a reasonable expectation of privacy," which include locations like restrooms, locker rooms, changing areas, and medical examination rooms. This is critical, since it is unclear whether wearable recordings would exist outside the scope of the state's preexisting peeping-tom statute, since the wearable itself is not generally hidden.
>
> The bill would also outlaw the practice of disabling indicators on wearable devices, or offering the means to do so. This is directly responsive to the fact that Meta's primary safety control, a small LED that illuminates when users take photos or videos, is easily disabled. For example, recent reports have identified individuals who offer to modify Meta glasses to disable the LED for as little as $60.
>
> [. . .]
>
> Unfortunately, we cannot simply trust technology companies to err on the side of restraint. Despite the recent bad news, Meta reportedly plans to reintroduce a controversial facial

recognition feature to its smart glasses, citing a "dynamic political environment where many civil society groups that we would expect to attack us would have their resources focused on other concerns."10 This feature would allow any glass-wearer to instantaneously identify any other passerby, possibly associating each identified person with a tranche of other personal information, including details sourced from social media or elsewhere. Put bluntly, wearable devices equipped with such facial recognition tools would effectively obliterate any remaining semblance of privacy that Californians are able to enjoy in public places. We strongly urge the committee to consider additional legislation to address this grave threat.

Ultimately, this bill should be viewed as the important first step toward regulating a policy area in desperate need of closer attention. It would reinvigorate Californians' right to privacy in highly intimate places for the wearable era and would ideally pave the way for a fuller discussion of the significant remaining issues.

Also writing in support, the California Federation of Labor Unions, AFL-CIO argues:

Advances in wearable technology, including AI-enabled smart glasses that incorporate cameras, microphones, and real time data processing capabilities, are quickly becoming more common in everyday life. Because many of these devices resemble ordinary eyewear, individuals may be unknowingly recorded, analyzed, or surveilled without their knowledge or consent, creating serious new privacy concerns.

Wearers of AI-enabled glasses can surreptitiously record workers, often in restaurants, retail, and hospitality, and expose their identities and interactions publicly without consent. A recent *New York Times* article detailed several examples of "food influencers" recording food service workers and restaurant owners without their knowledge. One video, recorded in Victorville, California without worker or customer permission, got 2 million views online.

These incidents expose workers to potential harassment, online comments, and unwanted visibility. It also can expose individuals' location and other details of their lives without permission, not just to the person recording, but all viewers online if posted. Immigrant workers, victims of domestic violence, and those who just want privacy are all put at risk by secret recordings, especially when those videos are posted online, exposing individuals to harassment by federal authorities or abusers.

California's existing privacy laws were developed before the emergence of these technologies and do not adequately address devices that can discreetly capture audio and video in real time. In many cases, current law assumes that recording devices are clearly visible or that individuals will receive meaningful notice that recording is occurring. However, wearable devices challenge these assumptions by embedding recording capabilities into everyday accessories that are difficult for bystanders to detect.

ARGUMENTS IN OPPOSITION: In opposition to the bill, a coalition of business associations led by TechNet argues:

Overbroad Definition Continues to Create Unintended Liability for Manufacturers

SB 1130 defines a "wearable recording device" broadly to include any device designed to be worn on or attached to the body that has the capacity to make sound or video recordings or transmit data to another device or the internet. In practice, this definition continues to

encompass a wide range of everyday consumer technologies, including action cameras, body-mounted tablets, and other wearable devices, that consumers use for entirely lawful and innocuous purposes.

This concern is especially significant for the restaurant and hospitality sectors, where workers regularly use wearable communication devices like earpieces and headsets to coordinate service and communicate with colleagues across a venue. Modern devices have mostly shifted from traditional radio signals to transmitting data via WiFi or internet. According to the bill's current wording, any device "designed to be worn on or attached to the body" that can "make sound or video recordings or transmit data ... to another device or the internet" would be classified as a wearable recording device, even if its primary use is only transmitting voice communications among staff. This could make hospitality employers and workers liable under criminal or civil law simply for using essential communication tools to serve customers, which clearly contradicts the bill's intended purpose.

Because existing provisions of the Penal Code define "person" to include business entities, and because the bill prohibits a "person" from "operating" such a device without defining the term "operate," the bill could have the unintended consequence of exposing device manufacturers to criminal and civil liability for the independent actions of their customers. Given the broad, ordinary meaning of "operate," and the fact that a manufacturer may control how a device functions, including, in some cases, how recorded data is transmitted or stored, a prosecutor or private litigant could argue that the manufacturer is "operating" the device whenever a customer uses it to capture sound or video. A manufacturer of an action camera or similar device, however, has no practical ability to control whether or how a purchaser uses that device in public or private settings.

This is particularly significant given the bill's private right of action. Imposing liability on a business for conduct it cannot control would represent a significant departure from the well-established principle that responsibility for unlawful recording should rest with the individual who chooses to engage in that conduct — the wearer — not the business that manufactured or sold the device.

Liability Should Attach to the User, Not the Manufacturer

The bill would be more appropriately tailored by clarifying that liability applies to the individual actually using the device to record audio or video, the wearer, rather than to a business that simply manufactures or sells the device.

Absent this clarification, SB 1130 risks sweeping in a broad range of entities far removed from the conduct the bill seeks to regulate and lacking the practical ability to prevent misuse.

New Anti-Circumvention Provisions Rely on an Unworkable "Primary Purpose" Standard

We recognize that the provisions addressing technology designed to disable a wearable recording device's indicator light are intended to target a different category of conduct than the core recording prohibition, and we do not object to liability attaching broadly to those who manufacture, sell, or use such circumvention technology. However, the standard the bill uses to define this conduct is unworkable as drafted.

Section 22949.86 prohibits manufacturing, selling, or offering for sale any technology "designed for the primary purpose of, marketed primarily for, or likely primarily used for" disabling a device's recording indicator. This "primary purpose" and "primarily marketed" framing introduces substantial uncertainty into an already difficult standard.

A retailer has no reliable way to evaluate whether a disabling feature is a primary or merely secondary design purpose of a product it sells. Similarly, a manufacturer or distributor has no practical way to determine whether a downstream retailer's marketing of a device will "primarily" emphasize a disabling feature it did not design or control. Businesses operating in good faith should not face civil penalties based on a standard this subjective and difficult to apply in practice.

We recommend that the Legislature replace this standard with a knowledge-based requirement, for example, liability should attach only where a person knowingly manufactures, sells, or distributes a product for the specific purpose of enabling the disabling of a recording indicator. A knowledge standard would preserve the bill's intent to prevent misuse.

"Reasonable Expectation of Privacy" Standard Remains Unclear and Unworkable

SB 1130 continues to prohibit recording in any area within a "place of business" as defined broadly as any office or retail establishment open to members of the public where a person has a "reasonable expectation of privacy." Neither term is defined with the specificity necessary to provide fair notice of what conduct is prohibited, and the combination of an expansive "place of business" definition with an undefined privacy standard creates genuine uncertainty even for everyday, well-intentioned conduct.

Consider a few examples. A patient in a doctor's office waiting room records a card game with a family member while waiting, and the recording incidentally captures another patient seated in the background. The waiting room is unquestionably a "place of business," and the other patient may well believe they have a reasonable expectation of privacy there, but it is not clear whether the outcome would differ if the same recording occurred in a hallway near treatment rooms rather than the waiting room itself.

Or consider a fitness studio that conducts weigh-ins on the sidewalk outside its entrance before class. The sidewalk may be the studio's property and thus a "place of business," and a participant being weighed, in view of a scale display, may believe they have a reasonable expectation of privacy in that moment. Would a passerby recording their daily commute for a personal video log be liable if their device incidentally captures that participant?

These are not far-fetched hypotheticals. They are the kinds of everyday situations this bill's current standard cannot reliably answer. This lack of clarity is especially concerning in a bill that imposes criminal penalties. California's existing criminal laws addressing non-consensual recording in sensitive contexts are, by contrast, drafted with considerable specificity.

REGISTERED SUPPORT / OPPOSITION:

Support

California Civil Liberties Advocacy
California Federation of Labor Unions, Afl-cio
Consumer Reports
Oakland Privacy

Oppose

Calchamber
California Restaurant Association
Computer and Communications Industry Association
Technet

Analysis Prepared by: Julie Salley / P. & C.P. / (916) 319-2200