Date of Hearing: June 23, 2026
Counsel: Mary Kennedy

ASSEMBLY COMMITTEE ON PUBLIC SAFETY
Nick Schultz, Chair

SB 1130 (Reyes) – As Amended June 16, 2026

SUMMARY: Prohibits a person from operating a wearable recording device within a place of business where a person has a reasonable expectation of privacy without consent of the person being recorded. Specifically, **this bill**:

1) Makes it a misdemeanor, punishable by imprisonment of up to one year and a fine of up to $1,500, for a person to 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.

2) 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.

3) Makes it a misdemeanor, punishable by imprisonment of up to one year and a fine of up to $1,500, for a person to disable any light sound or other indicator on a wearable recording device that indicates that the device is capturing sound or video.

4) Defines "place of business" as "any physical office or retail establishment in which members of the public receive goods or services from the business."

5) Defines "wearable recording device" as "any device that can 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."

6) 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.

7) 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.

8) 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.

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

10) Prohibits a person or entity from manufacturing, selling, delivering, holding, or offering for sale in commerce in this state 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. A violation is punishable by a civil penalty with a fine of $2,500 per violation.

11) Prohibits a person from purchasing, trading for, or otherwise acquiring any technology described above. A violation is punishable by a civil penalty with a fine of $2,500 per violation.

12) 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. A violation is punishable by a civil penalty with a fine of $2,500 per violation.

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

EXISTING LAW:

1) Makes it an alternate felony-misdemeanor, also known as a "wobbler," for any person to intentionally tap or make any unauthorized connection into a telephonic communication system (wiretapping) without the consent of all parties. (Pen. Code, § 631, subd. (a).)

2) Makes it a wobbler for a person to, intentionally and without the consent of all parties to a confidential communication, use an electronic amplifying and recording device to eavesdrop upon or record the confidential communications. (Pen. Code, § 632, subd. (a).)

3) Makes it a wobbler for a person to, maliciously and without the consent of all parties to the communication, intercept, receive, or assist in intercepting or receiving a communication transmitted between cell phones or between any cell phone and a landline phone. (Pen. Code, § 632.5, subd. (a).)

4) Makes it a wobbler for a person to, maliciously and without the consent of all parties to the communication, intercept, receive, or assist in intercepting or receiving a communication transmitted between cordless phone, between any cordless phone and a landline phone, or between a cordless phone and a cell phone. (Pen. Code, § 632.6, subd. (a).)

5) Makes it a wobbler for a person who, without the consent of all of the parties to a communication, intercepts or receives and intentionally records, or assists in the interception or reception and intentional recordation of, a communication transmitted between two cell phones, a cell phone and a landline phone, two cordless phones, a cordless phone and a landline phone, or a cordless phone and a cell phone. (Pen. Code, § 632.7, subd. (a).)

6) Includes elevated penalties when a person is convicted under one of the wiretapping, eavesdropping, or unlawful recording statutes and has a prior conviction for violating one of

the specified eavesdropping or unlawful recording statutes. (Pen. Code, §§ 631, 632, 632.5, 632.6, 632.7.)

7) Provides that the wiretapping, eavesdropping, and unlawful recording statutes do not prohibit the Attorney General, any district attorney, or any assistant, deputy, or investigator of the Attorney General or any district attorney, any officer of the California Highway Patrol, any peace officer of the Office of Internal Affairs of the Department of Corrections and Rehabilitation, any chief of police, assistant chief of police, or police officer of a city or city and county, any sheriff, undersheriff, or deputy sheriff regularly employed and paid in that capacity by a county, police officer of the County of Los Angeles, or any person acting pursuant to the direction of one of these law enforcement officers acting within the scope of their authority, from overhearing or recording any communication that they could lawfully overhear or record prior to January 1, 1968. (Pen. Code, § 633, subd. (a).)

8) Provides that the wiretapping, eavesdropping, and unlawful recording statutes do not prohibit any person regularly employed as an airport law enforcement officer acting within the scope of their authority from recording any communication which is received on an incoming phone line and for which the person initiating the call utilized a phone number known to the public to be a means of contacting airport law enforcement officers. (Pen. Code, § 633.1, subd. (a).)

9) Provides that the wiretapping, eavesdropping, and unlawful recording statutes do not prohibit one party to a confidential communication from recording the communication for the purpose of obtaining evidence reasonably believed to relate to the commission by another party to the communication of the crime of extortion, kidnapping, bribery, or any felony involving violence against the person. (Pen. Code, § 633.5.)

10) Creates a wobbler for any person who trespasses on property for the purpose of committing or attempting to commit any act, in violation of the wiretapping, eavesdropping, or unlawful recording statutes. (Pen. Code, § 634.)

11) 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, subd. (j)(3)(A).)

12) 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*.)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Sponsor:** Author Sponsored

2) **Author's statement:** "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 indicator lights 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."

3) **Existing Laws Related to Wiretapping and Eavesdropping:** Penal Code section 630 declares that "advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." However, existing law also "recognizes that law enforcement agencies have a legitimate need to employ modern listening devices and techniques in the investigation of criminal conduct and the apprehension of lawbreakers." (*Ibid*.)

   Penal Code sections 631-632.7 set forth a comprehensive statutory scheme protecting the right of privacy by prohibiting unlawful wiretapping and other forms of illegal electronic eavesdropping. Unless a specific exception applies, a person may not intercept, record, or listen to confidential communications whether on a conventional, cordless, or cell phone. Penal Code section 633 outlines a major exemption to the prohibition on unlawful wiretapping and electronic eavesdropping: [The prohibitions on wiretapping and eavesdropping] do not prohibit the Attorney General, any district attorney, or any assistant, deputy, or investigator of the Attorney General or any district attorney, any officer of the California Highway Patrol, any peace officer of the Office of Internal Affairs of the Department of Corrections and Rehabilitation, any chief of police, assistant chief of police, or police officer of a city or city and county, any sheriff, undersheriff, or deputy sheriff regularly employed and paid in that capacity by a county, police officer of the County of Los

Angeles, or any person acting pursuant to the direction of one of these law enforcement officers acting within the scope of their authority, from overhearing or recording any communication that they could lawfully overhear or record prior to January 1, 1968.

Penal Code section 633.1 similarly exempts airport law enforcement officers. Finally, Penal Code section 633.5 provides that the wiretapping and eavesdropping statutes do not prohibit a party to a confidential communication from recording the communication for the purpose of obtaining evidence reasonably believed to relate to the commission by another party to the communication of extortion, kidnapping, bribery, or any felony involving violence against the person.

4) **Emerging Technology and Consumer Products Are Creating New Privacy Concerns:** Smart glasses are eyewear that can correct vision and offer additional features not present in traditional eyewear, including camera functions for photography and video recording, AI capabilities, and integration with other devices.[1] Although smart glasses have existed for years, they began to gain popularity following Meta's release of its Ray-Ban Stories product in 2021.[2]

   The increased popularity of these products and the ability to surreptitiously record others has received a significant amount of attention in recent months.[3]

   One anecdote involved an individual who realized that her esthetician was wearing smart glasses with recording capabilities during a waxing appointment.[4]

5) **Addressing Privacy Concerns:** This bill seeks to address privacy concerns related to surreptitious recordings using devices such as smart glasses and contains two major components. The first component prohibits operating 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, and prohibits a person from disabling any light or other device on a wearable recording device that indicates that the device is capturing sound or video. The penalty would be an enhanced misdemeanor punishable by up to one year in jail and a fine not exceeding $1,500. The bill also makes it a misdemeanor to disable any light, sound, or other indicator on a wearable device that indicates the device is capturing sound or video.

---

[1] Hornby, *What are smart glasses? Yesteryear's 'next big thing' is finally finding an audience* (Jul. 10, 2024). <https://www.laptopmag.com/gaming/vr/what-are-smart-glasses>.
[2] Hector, *The Ray-Ban Meta smart glasses are majorly popular, which is exciting and frightening in equal measure* (Oct. 21, 2024) <https://www.techradar.com/computing/virtual-reality-augmented-reality/the-ray-ban-meta-smart-glasses-are-majorly-popular-which-is-exciting-and-frightening-in-equal-measure>.
[3] See Greenwald, *Are You Being Secretly Recorded by Smart Glasses? Here's How to Tell* (Mar. 4, 2026) <https://www.pcmag.com/explainers/are-you-being-secretly-recorded-by-smart-glasses-heres-how-to-tell>; Dellinger, *Dear Meta Smart Glasses Wearers: You're Being Watched, Too* (Mar. 3, 2026) <https://gizmodo.com/dear-meta-smart-glasses-wearers-youre-being-watched-too-2000728928>; Chun, *How to Tell if Someone Is Filming You With Smart Glasses* (Mar. 15, 2026) <https://www.cnet.com/tech/mobile/how-to-identify-smart-glasses/>; Fortney, *Dinner Is Being Recorded, Whether You Know It or Not* (Feb. 16, 2026) <https://www.nytimes.com/2026/02/16/dining/meta-ray-ban-glasses-restaurants.html>.
[4] Prada, *Woman Accuses Tech of Wearing Meta Recording Glasses During Her Brazilian Wax* (Sept. 2, 2025) <https://www.vice.com/en/article/woman-accuses-tech-of-wearing-meta-recording-glasses-during-her-brazilian-wax/>.

The bill specifically provides that recording a public officer or peace officer while the office of the public place or the person is in a place they have the right to be does not in and of itself constitute a violation of these provisions nor does it provide a basis for detaining or arresting an individual.

The bill states that it does not apply to a body worn camera when used by a public officer or a peace officer in the performance of their duties nor does it apply to hearing aids, augmentative and alternative communication devices when used for overcoming hearing impairment.

The second component makes it a civil violation to manufacture, sell, deliver, hold or offer for sale any technology 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, and prohibits the purchase and acquisition of that technology.

This bill defines "wearable recording device" as "any device that can 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," and "place of business" as "any physical office or retail establishment in which members of the public receive goods or services from the business."

This bill also adds the new Penal Code section created by this bill to the provisions allowing law enforcement to surreptitiously record under specified circumstances.

The author and supporters believe that this bill protects privacy concerns in places where people have an expectation of privacy while allowing law enforcement and the public to record when appropriate.

6) **Argument in Support:** According to the *California Federation of Labor Unions, AFL-CIO*, "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.

"SB 1130 takes an important step toward closing this gap in the law. The bill defines wearable recording devices and establishes clear rules to ensure transparency and accountability when these technologies are used. Specifically, the measure prohibits recording using these wearable devices in areas within places of business where individuals have a reasonable expectation of privacy without explicit consent. It also prohibits tampering with or disabling recording indicator lights that notify others when recording is taking place.

"These protections are especially important for communities that may already face heightened risks of harassment, stalking, or surveillance. By establishing clear standards for transparency and consent, SB 1130 helps ensure that emerging technologies do not erode Californians' fundamental right to privacy."

7) **Argument in Opposition:** According to *TechNet,* "TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of American innovation by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes more than 100 dynamic American businesses ranging from startups to the most iconic companies on the planet and represents five million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

"We appreciate the author's intent to protect individuals' privacy and prevent non-consensual recording in sensitive environments. However, as drafted, SB 1130 raises significant concerns regarding overbreadth, unclear standards, and the imposition of liability on entities that lack the ability to control user behavior.

"**Overbroad Definition Creates Unintended Liability for Businesses**

"SB 1130 defines a "wearable recording device" broadly to include any device worn on or attached to the body that can capture or transmit audio or video.

"In practice, this definition could encompass a wide range of everyday consumer technologies, including smartphones, tablets, and action cameras. Because existing provisions of the Penal Code define "person" to include business entities, the bill could have the unintended consequence of exposing manufacturers and other businesses to criminal and civil liability for the actions of end users.

"Further, the bill prohibits a "person" from "operating" such a device in certain contexts but does not define the term "operate." Given its broad, ordinary meaning, this could be interpreted to extend liability beyond the individual user to entities involved in the design, manufacture, or distribution of devices.

"Businesses that manufacture or sell these devices have no control over how individual consumers use them in public or private settings. For example, an action camera or tablet manufacturer cannot control whether a purchaser uses a device to capture audio or video in a location where another individual may have a reasonable expectation of privacy.

"Imposing liability under these circumstances would represent a significant departure from established principles that assign responsibility to the individual engaging in the conduct at issue.

"**Unclear "Reasonable Expectation of Privacy" Standard and Increased Litigation Risk**

"SB 1130 prohibits recording in areas within a place of business where a person has a "reasonable expectation of privacy," but does not clearly define which locations fall within this category.

"Places of business vary widely, and there is no clear, actionable standard for determining where such expectations apply. Without further specificity, individuals and businesses alike may struggle to understand when recording is permitted. This ambiguity creates a risk that the bill could be interpreted as prohibiting the use of commonplace devices across a broad range of everyday settings.

"Furthermore, because the bill establishes new violations tied to broadly defined conduct and ambiguous standards, it may lead to significant enforcement challenges and increased litigation. Even if liability were limited to individual users, the lack of clear boundaries could expose ordinary Californians to potential penalties for routine use of devices in public-facing environments.

"**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.

"**A Targeted Approach Is Available**

"California law already includes carefully tailored prohibitions addressing non-consensual recording in sensitive contexts, including specific restrictions related to recording individuals in private settings or while engaged in intimate activity. A more effective and balanced approach would be to build on these existing frameworks by clearly identifying the specific contexts in which recording is prohibited and ensuring that liability attaches to the individual engaging in the prohibited conduct.

"Providing this level of clarity would better align the bill with its stated intent while avoiding unintended consequences for consumers and businesses.

"While we share the goal of protecting individuals' privacy, SB 1130, as drafted, raises significant concerns related to overbreadth, unclear standards, and unintended liability for businesses that cannot control how their products are used."

8) **Prior Legislation**

a) AB 1962 (Berman), Chapter 367, Statutes of 2024, prohibited recordings or transcriptions of smart speaker devices.

b) SB 1272 (Becker), Chapter 27, Statutes of 2022, clarified that the exemption from wiretapping for maintenance and operation purposes, applies to a telephone company as well as a utility.

c) AB 2669 (Jones-Sawyer), Chapter 175, Statutes of 2018, added peace officers of the Office of Internal Affairs of the Department of Correctional and Rehabilitation to the list of law enforcement officers who may eavesdrop or record communications.

d) AB 324 (Kiley), Chapter 246, Statutes of 2018, defined identifiable for the purposes of prohibiting surreptitiously recording an identifiable person under or through their clothing.

e) AB 413 (Eggman), Chapter 191, Statutes of 2017, allowed a party to a confidential communication record the communication for the purpose of obtaining evidence reasonably believed to relate to domestic violence and provides that such evidence is not inadmissible in prosecution against the perpetrator of the domestic violence.

f) AB 1671 (Gomez), Chapter 855, Statutes of 2016, made it a wobbler to intentionally distribute, or aid and abet the distribution of, a confidential communication with a health care provider that was obtained unlawfully.

g) AB 2645 (Connelly), Chapter 298, Statutes of 1992, expanded the surreptitious recording of telephones to apply to cell phones.

h) AB 860 (Unruh), Chapter 1509, Statutes of 1967, made California a two-party consent state prohibiting the recording of confidential communications without express permission of all parties.

REGISTERED SUPPORT / OPPOSITION:

Support

California Civil Liberties Advocacy
California Federation of Labor Unions, Afl-cio
Cft – a Union of Educators & Classified Professionals, Aft, Afl-cio
Consumer Reports
Oakland Privacy

Opposition

Cal Chamber
California Chamber of Commerce
California Restaurant Association
Computer & Communications Industry Association
Computer and Communications Industry Association
Technet

Analysis Prepared by: Mary Kennedy / PUB. S. / (916) 319-3744