
CALIFORNIA PRIVACY PROTECTION AGENCY

400 R ST. SUITE 350
SACRAMENTO, CA 95811
cppa.ca.gov



Date: October 12, 2026

To: California Privacy Protection Agency Board
(Meeting of November 6, 2026)

From: Maureen Mahoney
Deputy Director of Policy & Legislation

Subject: Agenda Item 5 – Legislation Update and Agency Proposals

This memorandum provides for the California Privacy Protection Agency Board's consideration several bill ideas that would address emerging privacy issues and improve privacy for Californians. These ideas seek to address issues that Board Members and staff have flagged for attention, amend existing laws to increase privacy protections, and improve transparency and accessibility.

Staff requests Board feedback on these ideas and Board guidance on what staff is authorized to present to members of the California legislature for possible authoring and Agency support. Because the decision to sponsor a bill depends on several factors, such as the subject matter of the bill, the amount of work that the specific bill would require, and whether the author has identified other sponsors for the bill, staff recommends that the Board provide directional feedback while leaving it to staff's discretion whether to sponsor any ideas discussed below.

Tier 1 outlines a bill proposal on wearables, as multiple Board Members have expressed interest in this area of focus. Staff recommends that the Board support the proposal. If so, subject to the Board's delegation, staff could determine that the Agency should sponsor the proposed legislation. Sponsorship typically involves working closely with a legislator to draft the bill and engaging with stakeholders to shape the bill as it proceeds through the legislative process, along with communicating the Agency's position to the legislature.

Tier 2 of the memo outlines proposals or policy areas that the Board may want to identify as a priority, but, subject to the Board's determination, Agency may not be in the best position to sponsor legislation at this time. Staff would provide updates on any legislation introduced in this area, including at the February board meeting, and the Board could consider taking positions on bills that have emerged in these areas in May. If the Board votes to support such bills in future meetings, staff would provide technical assistance to the author as the bill moves through the legislative process and communicate the Agency's position to the legislature.

Finally, we note in Tier 3 that there may be a number of important bills reintroduced next year that we have previously supported, such as AB 1542 (Ward), which prohibited the sale or sharing of sensitive personal information, and SB 435 (Wahab), which narrowed the publicly available information exemption in the California Consumer Privacy Act (CCPA). Since we expect that there will be a large number of important privacy and AI-related bills to bring before the Board next year, we anticipate that staff will only have the resources to sponsor up to one proposal.

TIER 1

Prohibition on Facial Recognition Technology in Wearable Recording Devices

Wearable recording camera devices, such as smart glasses and body cameras, have moved from novelty products with limited use cases to mainstream consumer technology and their increasing use in everyday life raises novel privacy concerns.

First, new consumer-oriented wearable cameras are often small and inconspicuous, complicating existing understandings of notice and control for people who are the targets of recording. A handheld phone camera, for example, requires the user to aim it at someone which creates noticeable intent that is subject to social norms. Wearable cameras built into everyday fashion items remove that social friction because recording can happen without the wearer ever physically indicating that they are recording. The risk shifts from a noticeable, occasional one to a potentially universal one that follows anyone who enters a public space. Additionally, because this wearable technology is now often marketed and designed as ordinary eyewear, targets may not know who is equipped with a camera, leaving them unable to take basic precautions like avoiding obvious recording or opting out of an interaction or location that is known to be recorded. For example, Amazon intends to equip 20,000 drivers with smart glasses by 2027 that will take photos "almost constantly" as they make delivery rounds and send those images back to an AI database with no option for customer opt-out.¹

Second, because of their inconspicuous and portable nature, these devices also increase the likelihood of widespread facial recognition and surveillance. For example, in 2024, two Harvard students built a facial recognition system that they paired with Meta's Ray-Ban smart glasses that allowed them to take video of strangers on the street and find personal information about the individuals within seconds without the subjects' knowledge or consent.² The students noted that the subjects did not notice the recording indicator lights on the smart glasses even when they had conversations with them. Additionally, more recent reporting indicated that wearable companies have explored building similar facial recognition features directly into smart glasses and their connected technology platforms.³

If facial recognition is built into these wearables, the risk of harm would increase exponentially, and privacy regulations would be playing catch up. The potential for covert surveillance, harassment, and unauthorized data collection would extend to anyone who walks past the wearer. An abusive ex-partner, stalker, harasser, or bad faith actor would gain a discreet tool for locating, tracking, and gathering information on a person that previously required significant effort, technical skill, or access to specialized equipment or software. Additionally, wearable companies would hold recorded data incorporating detailed sensitive data on countless individuals that would be vulnerable to unauthorized access, misuse, or breach without their knowledge.

Existing privacy laws are not adequate to address these concerns. The CCPA, for example, requires businesses that control collection of personal information to provide notice to consumers at or before the time of collection about what information will be collected, how it will be used, and whether the information will be shared with third parties, yet this disclosure will not give notice to the unknowing subject of a wearable recording. The law also gives consumers the right to have the data deleted, to stop the sale or sharing of the data, or to limit the use and disclosure of sensitive personal information, such as biometric data, but these rights may not be

¹ Bonifield, Stevie, *Amazon's delivery driver smart glasses will reportedly take photos 'almost constantly,'* The Verge (September 30, 2026) <https://www.theverge.com/tech/1002766/amazon-delivery-driver-smart-glasses-privacy>

² Hill, Kashmir, *Two Students Created Face Recognition Glasses. It Wasn't Hard,* NY Times (October 24, 2024) <https://www.nytimes.com/2024/10/24/technology/facial-recognition-glasses-privacy-harvard.html>

³ Cameron, Dell & Dhruv Mehrotra, *Meta Silently Added Face-Recognition Code for Its Smart Glasses to Millions of Phones,* Wired (June 4, 2026) <https://www.wired.com/story/meta-smart-glasses-face-recognition-nametags-connections/>

useful to an individual who is unaware they have been captured and identified by a wearable device. Similarly, state laws, like Illinois' Biometric Information Privacy Act and Washington's My Health My Data Act,⁴ that require opt-in consent for the collection of biometric data also do not take into account that when a wearable is used the business may collect personal information of a recorded subject through an intermediary (the person wearing the glasses). Legislation is needed to address this gap to ensure that those being recorded are properly protected.

Amending the CCPA to prohibit the collection or use of biometric data by consumer wearable recording devices and prohibiting the integration of facial recognition technology with wearable recording devices would limit real time facial recognition capabilities and minimize some of the privacy risks associated with these devices. Consumers would still be able to use the wearable device to capture real-time footage, however the device and the connected technologies offered by the business would not be able to use the data in the images for the purpose of identification. Such a restriction would maintain important levels of friction and existing reasonable expectations of privacy.

Earlier this year, the California legislature passed a bill addressing privacy concerns related to wearable recording devices (SB 1130, Reyes) that was vetoed by the Governor.⁵ The bill required that manufacturers of wearable recording devices include indicators that recording is occurring, prohibited individuals from disabling recording indicators, and prohibited recording in a place of business where an individual would have a reasonable expectation of privacy, among other things. In his veto message, the Governor expressed concern that the definition of wearable recording device was overly broad, potentially including consumer technology such as smart watches, and that the recording prohibition was already adequately addressed by existing law.⁶

Opponents of the bill also expressed concerns that the scope of the bill may have been too broad in certain circumstances. For example, technology companies and restaurant associations were concerned that the prohibition on recording could sweep in work-related devices like action cameras or restaurant headsets that could be used for lawful or innocuous purposes.⁷ Additionally, disability advocacy organizations raised concerns that the bill would prevent the use of wearables as assistive technology for people with disabilities.⁸

To address these concerns, the proposal could include exceptions to ensure that the restriction would not limit (1) the use of assistive technology by individuals with disabilities that are used for the purpose of supporting a person's functional needs related to the disability or condition, (2) the use of biometric information for the purpose of securing a personal mobile device, and (3) identifying technology used by employers to monitor employee access to work facilities.

Recommendation: Staff recommends that the Board approve this proposal and direct staff to present this to members of the California legislature for possible authoring and Agency support. Because the decision to sponsor a bill depends on several factors, such as the amount of work that the specific bill would require, whether the author has identified other sponsors for the bill,

⁴ 740 ILCS Sec 14/1 et seq; Wash. Rev. Code Sec. 19.375.010 et seq.

⁵ SB 1130, 2025-2026 Leg., Reg. Sess. (Cal 2026), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260SB1130

⁶ Cal. Gov. Gavin Newsom, Veto Message for Senate Bill 1130 (Sept. 30, 2026), <https://www.gov.ca.gov/wp-content/uploads/2026/09/VETO-msg-SB-1130.pdf>

⁷ Assembly Committee on Privacy and Consumer Protection, Bill Analysis for SB 1130 (Reyes), June 28, 2026

⁸ Decker, John W., *California can protect privacy without limiting tech that helps people with disabilities work*, Capitol Weekly (September 29, 2026) <https://capitolweekly.net/california-can-protect-privacy-without-limiting-tech-that-helps-people-with-disabilities-work/>

or wants the bill to be author-sponsored, staff recommends leaving it to staff's discretion whether to sponsor the proposal.

TIER 2

Require Opt-In Consent for the Processing of Personal Information to Train AI Models

Generative AI models are systems that produce content based on inputs they are given. The ability to produce an output is a result of model training, where the system is exposed to large quantities of data so that it can learn patterns and connections from the data that allow it to make predictions and produce new content. The model does not store each individual piece of data and then provide that specific data in response to a request; rather, it is able to use the connections and patterns it learned from the data to produce the requested output. Models are trained on large datasets and then often fine-tuned with additional data sets to improve performance in more specialized areas.⁹

Generative AI models, such as large language models, must be trained on enormous amounts of data. While much of the data may be sourced from the internet or licensed datasets, it increasingly includes personal information collected from user interactions with AI products or consumer data provided in one context that is then transferred to a model developer to be used as training data.¹⁰ The consumer data often includes personal information such as names, contact details, health disclosures, location data, financial circumstances, and private correspondence. Training an AI system on this personal data takes it out of its original context and repurposes it in ways the individual may not have anticipated or intended.

Additionally, consumers increasingly provide significant amounts of sensitive personal information to AI chatbots and AI agents. For example, people are often very forthcoming with chatbots and share information about illnesses, mental health concerns, and relationships. A recent review of the privacy policies of the most popular AI chatbots showed that most of these platforms allow for this conversation data to be used to train the AI system by default.¹¹ Similarly, to effectively use an AI agent, consumers often have to provide the agent with extensive access to highly personal information like financial accounts, health records, regularly used apps, contact lists, email accounts, and calendar systems.¹²

The growing interest in these new consumer AI products, however, does not necessarily mean that consumers understand or consent to their data being used to train AI models. In 2024, for example, LinkedIn began training its AI using account holders' information without giving users adequate notice and there was significant backlash.¹³ Many consumers were frustrated that there was not advanced notice or opportunity to opt-out before their data was used for training purposes. Employees, too, have expressed concerns about the potential use of their data to train AI systems. Former Spirit Airlines flight attendants and pilots have resisted Google's efforts

⁹ Congressional Research Service, *Generative Artificial Intelligence and Data Privacy: A Primer*, R47569 (May 23, 2023) <https://www.everycrsreport.com/reports/R47569.html>

¹⁰ King, Jennifer, et al, *User Privacy and Large Language Models: An Analysis of Frontier Developers' Privacy Policies*, Stanford (September 2025) <https://arxiv.org/pdf/2509.05382>

¹¹ *Id.*

¹² Tan, Eli, *I Gave My Life Over to Meta's AI Agent and Was Blown Away*, NY Times (September 22, 2026) <https://www.nytimes.com/2026/09/22/technology/meta-muse-ai-agent.html>

¹³ Velazco, Chris, *LinkedIn is training AI on you – Unless you opt-out with this setting*, Washington Post (Sept. 23, 2024) <https://www.washingtonpost.com/technology/2024/09/23/linkedin-training-ai-setting-opt-out/>

to purchase their data at auction for AI training purposes.¹⁴

The risks go beyond the initial collection. Research has shown that AI models can reproduce portions of their training data when prompted. Researchers have been able to extract names, phone numbers, and email addresses from public AI models.¹⁵ Indeed, even when safety measures are built into a foundational model to prevent leakage, studies have shown that fine-tuning done later to specialize a model for a new purpose can introduce vulnerabilities that make disclosure of personal information possible.¹⁶

Unfortunately, existing privacy rights do not adequately address these concerns. Once personal information has been used to train a model, it is very difficult to remove. The model itself does not retain the specific data, but a series of connections and patterns it learned from that data that become integrated with the other patterns it knows and uses to develop outputs.¹⁷

Amending the CCPA to require opt-in consent for the collection, use, and disclosure of personal information to train AI models would put consumers in control of their data and would minimize unwanted privacy risks. It would ensure that personal information enters training datasets only when the individual has been informed and affirmatively agreed. It would also clarify that use of an AI product does not imply consent to the use of personal information for model training. Additionally, an opt-in requirement could encourage AI developers and data providers to properly license data before any training uses and center privacy considerations in their model training programs.

California previously considered bills related to AI model development and training data that can highlight potential opposition for a bill requiring consent to collect, use, and disclose personal information to train AI models.¹⁸

- Earlier this year, the Legislature considered AB 2027 (Ward) which would have established prohibitions on the use of employee personal information to train AI systems intended to replicate or replace the employee's job. The bill was held in Assembly Appropriations. Tech and employer associations expressed concerns that the restriction would be unworkable and hinder innovation.¹⁹
- In 2025, California enacted SB 53 (Weiner) which requires developers of frontier AI models to publish safety frameworks and transparency reports, report critical safety incidents, and protect internal whistleblowers. This bill faced opposition from tech

¹⁴ Vlamis, Kelsey, *Google just got a boost in its bid to buy Spirit Airlines' data for AI training*, Business Insider (Oct. 5, 2026) <https://www.businessinsider.com/google-bid-spirit-airlines-data-ai-boost-official-recommended-approval-2026-10>

¹⁵ Nasr, et al, *Scalable Extraction of Training Data from (Production) Language Models* (November 28, 2023) <https://arxiv.org/pdf/2311.17035>; White, Jeremy, *How Strangers Got My Email Address from ChatGPT's Model*, NY Times (December 22, 2023) <https://www.nytimes.com/interactive/2023/12/22/technology/openai-chatgpt-privacy-exploit.html>.

¹⁶ Chen, et al, *The Janus Interface: How Fine-Tuning in Large Language Models Amplifies the Privacy Risks* (October 24, 2023) <https://arxiv.org/abs/2310.15469>; Lukas, et al, *Analyzing Leakage of Personally Identifiable Information in Language Models* (February 1, 2023) <https://arxiv.org/abs/2302.00539>

¹⁷ Pastis, Stephen, *A.I.'s un-learning problem: Researchers say it's virtually impossible to make an A.I. model 'forget' the things it learns from private user data*, Yahoo! Finance (Aug. 30, 2023) <https://finance.yahoo.com/news/un-learning-problem-researchers-virtually-164342971.html>; Layne, Rachel, *How to Make AI 'Forget' the Private Data it Shouldn't Have*, Harvard Business School Working Knowledge (February 22, 2024) <https://www.library.hbs.edu/working-knowledge/ga-seth-neel-on-machine-unlearning-and-the-right-to-be-forgotten>.

¹⁸ AB 2013, 2023-24 Leg., Reg. Sess. (Cal. 2024); SB 53, 2025-26 Leg., Reg. Sess. (Cal 2025); AB 2027, 2025-26 Leg., Reg Sess. (Cal 2026).

¹⁹ Assembly Committee on Privacy and Consumer Protection, Bill Analysis for AB 2027 (Ward), April 29, 2026.

associations and while the majority of their objections would not be applicable to this bill, there were some concerns about the scope and definition of frontier AI models that could come into play with this proposal.

- In 2024, California enacted AB 2013 (Irwin) which requires certain disclosures about the types of materials used for AI training. Tech industry opposition for that law was concerned about properly scoping the definition of terms such as “training” and “developer” for clarity and effectiveness.²⁰
- In 2024, California considered AB 2877 (Bauer-Kahan), which would have amended the CCPA to require AI developers to obtain opt-in consent for the use of the personal information of a child under 16 to train an AI model.²¹ The bill was held in Senate Appropriations. Tech industry opponents argued that limitations on AI training would limit business’s ability to train models to be more privacy protective or to prevent outcomes such as bias or discrimination.²²

Staff have developed this proposal in response to Board Members’ expressed interest in addressing agentic AI. The proposal seeks to ameliorate the risks posed in this space and is based on ideas that staff and the legislature have previously considered. Based on staff’s current thinking, this proposal would have value from a privacy perspective. However, agentic AI specifically is a new and emerging space, and further research would be necessary to develop a proposal to address this issue directly.

Further, given the extent of expected opposition to a proposal to require opt-in consent for the processing of personal information to train AI, it would require specialized coalition building, so staff would not be able to hit the ground running in 2027.

Recommendation: Direct staff to further research agentic AI and revisit the issue in 2027. Should bills relating to AI training or agentic AI be introduced in 2027, staff recommends that the Board consider supporting this or similar legislation.

Rein in Advanced Surveillance Technologies

The proliferation of Automated License Plate Reader (ALPR) technology, including provided by vendors such as Flock, has attracted increased public concern in recent months. While their use is not limited to law enforcement, some police departments use ALPR data to identify stolen vehicles or those associated with crimes. However, location data unknowingly collected from public surveillance technologies like cameras and automated license plate readers can create a detailed map of individual movement that reveals deeply personal information. Privacy advocates have raised concerns about the disclosure of ALPR information from law enforcement entities in California to other states and the federal government,²³ and the Washington Post has reported that dozens of law enforcement officials have been charged with or accused of unauthorized use of ALPR information, in some cases, to spy on their partners.²⁴

²⁰ Assembly Committee on Privacy and Consumer Protection, Bill Analysis of AB 2013 (Irwin), April 28, 2024.

²¹ AB 2877, 2023-24 Leg., Reg. Sess. (Cal. 2024).

²² Senate Judiciary Committee, Bill Analysis of AB 2877 (Bauer-Kahan), June 21, 2024.

²³ Letter from the Electronic Frontier Foundation et al. to Attorney General Bonta re: enforcing SB 34 on ALPRs (Jan. 31, 2024), <https://www.eff.org/document/01-31-2024-letter-california-ag-rob-bonta-re-enforcing-sb34-alprs>; Johnson, Khari and Mohamed Al Elew, *California police are illegally sharing license plate data with ICE and Border Patrol*, CalMatters (June 13, 2025), <https://calmatters.org/economy/technology/2025/06/california-police-sharing-license-plate-reader-data/>.

²⁴ Harwell, Drew et al., *How rogue officers turned a nationwide camera network into a tool for stalking*, Wash. Post (August 2, 2026), <https://www.washingtonpost.com/technology/2026/08/02/how-police-officers-used-vast-network-cameras-spy-their-exes/>.

Jurisdictions across the country have adopted new guardrails over the use of this data.²⁵

In 2015, California adopted SB 34 (2015), which prohibits public agencies from selling, sharing, or transferring ALPR data, except to another agency, and requires public agencies intending to operate an ALPR system to provide an opportunity for public comment before implementation, among other things.²⁶

Recent efforts by the California legislature to further regulate ALPR have been less successful. This year a bill, SB 1013, which would have established new regulations around government use of ALPR information, stalled in the final days of the legislative session.²⁷ It had faced opposition from law enforcement groups, which argued that the data retention limits in the bill would remove access to information important to solving crimes.²⁸ The bill would have, among other things:

- Allowed law enforcement to use ALPR only to locate vehicles or people when reasonably suspected of being involved in a public offense or to find someone reported missing;
- Required public agencies to archive all ALPR information that has been held for more than 60 days, unless the information is related to active investigation or criminal proceeding or matches information on a hot list;
- Prohibited a public agency from querying any archived information without a warrant.

The California legislature has also considered legislation in recent years to provide more control over businesses' collection and use of location information. AB 1355 (Ward), which was placed in a separate part of the Civil Code than the CCPA, would have put new retention limits on location information and prohibited its sale, including location information captured by an ALPR system.²⁹ The Board voted to support AB 1355 in 2025. The bill faced opposition from business groups, which opposed the bill's private right of action and argued that the bill would create confusion in its interaction with the CCPA.³⁰ Law enforcement groups also opposed the measure. After AB 1355 failed to pass out of its chamber of origin, the author then amended AB 322, which had passed the Assembly, in full to address how the CCPA regulated precise geolocation data.³¹ CalPrivacy also supported this bill, which ultimately stalled. Business groups also opposed this version of the bill, arguing that the notice requirements would impair the consumer experience.³²

While the legislature has considered a number of proposals related to ALPRs and location data more broadly, staff is not aware that it has yet considered a proposal to prohibit the use of facial recognition technology in ALPR systems. While Flock has vowed not to use FRT, another company, VIDIZMO, has advertised its potential ability to apply FRT to Flock footage.³³ This would pose additional privacy concerns to pedestrians who may inadvertently trigger and be

²⁵ Vigdor, Neil, *Flock Cameras Are Dividing U.S. Cities. Here's What to Know About Them*, NY Times (September 1, 2026) <https://www.nytimes.com/article/flock-safety-camera-technology.html>

²⁶ SB 34, 2015-26 Leg. Reg. Sess. (Cal. 2015), https://www.leginfo.ca.gov/pub/15-16/bill/sen/sb_0001-0050/sb_34_bill_20151006_chaptered.html

²⁷ SB 1013, 2025-26 Leg., Reg. Sess. (Cal. 2026), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260SB1013

²⁸ Assembly Committee on Privacy and Consumer Protection, Bill Analysis for SB 1013, June 28, 2026.

²⁹ AB 1355, 2025-26 Leg., Reg. Sess. (Cal. 2025), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260AB1355

³⁰ Assembly Judiciary Committee on Privacy and Consumer Protection, Bill Analysis for AB 1355, April 24, 2025.

³¹ AB 322, 2025-26 Leg., Reg. Session (Cal. 2025), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260AB322

³² Senate Judiciary Committee, Bill Analysis for AB 322, July 11, 2025.

³³ Jason Koebler, *Surveillance Company Tells Cops It Wants to Add Facial Recognition to Flock Camera*, 404 Media (Sept. 29, 2026), <https://www.404media.co/surveillance-company-tells-cops-it-wants-to-add-facial-recognition-to-flock-cameras/>

tracked by these systems without their knowledge or consent. A recent Executive Order signed by Missouri Governor Mike Kehoe prohibited the integration of FRT into ALPR systems,³⁴ and Sen. Josh Hawley (R-Mo.) plans to introduce a bill that would include a similar provision.³⁵ This could be an area that the Board may want to direct staff to explore.

Recommendation: Given Board Members' expressed interest in ALPR, the Board may want to identify this issue as a priority area. It is expected that ALPR will be an active topic in the California legislature in 2027. Should bills similar to those described above be reintroduced in 2027, staff recommends that the Board consider supporting this or similar legislation. If the legislature does not introduce legislation that achieves similar policy goals, staff recommends that the Board revisit the topic in February.

Require that Mobile Device and Connected TV Manufacturers Make Advertising IDs Accessible and Able to be Reset, and Deleted or Deactivated

Mobile apps accessed via mobile devices, connected TVs, and mobile streaming devices monitor online activity and collect personal information using the unique advertising IDs assigned to each device. Apps collect information about user activity paired with the unique advertising ID to place targeted ads seamlessly into the app experience. This collected information can also be sold and shared with third parties like data brokers or advertising platforms.

There is variation across mobile devices and connected TVs about how consumers can access and control the advertising ID and data collection by mobile apps for advertising purposes. For example, on Android mobile devices users can view their advertising ID in the Privacy Setting and either (1) delete it, which will stop all data tracking for advertising, or (2) reset it which disrupts data collection by restarting tracking under a new ID, minimizing long term collection. In contrast, on Apple mobile devices, by default apps are not allowed to access the advertising ID and must individually request permission from the consumer to access the ID. Apple does not make the ID visible to the user but offers a setting that will automatically deny all app tracking requests preventing app level tracking all together and rendering the ID nonfunctional.³⁶

There is a similar distinction among connected TVs and mobile streaming devices. For example, the Apple TV mobile streaming device functions similarly to its mobile device — by default apps are not allowed to access the advertising ID and must individually request permission to track the user. The ID is not made visible to the user. Other TV platforms like Google TV, Amazon Fire TV, and Roku give consumers the option to reset or delete the ID. It appears that these platforms make the ID visible in the settings but that is difficult to confirm given the volume of TV models. In contrast, the Samsung Tizen OS does provide the ID, but according to some sources appears to only give consumers the option to reset the ID, not to delete it. Additionally, LG TVs appear to have advertising tracking off by default and offer consumers the opportunity to opt-in during set-up. It is unclear if the advertising ID is made visible to consumers in the LG TV platform.³⁷

³⁴ Governor Kehoe, *Governor Kehoe Signs Executive Order Establishing Safeguards on Automated License Plate Readers* (Sept. 16, 2026), <https://governor.mo.gov/press-releases/archive/governor-kehoe-signs-executive-order-establishing-safeguards-automated>

³⁵ Senator Josh Hawley, *Hawley to Introduce Stop Flock Abuse Act, Establishing Safeguards for Ai-Powered Cameras* (Sept. 30, 2026), <https://www.hawley.senate.gov/hawley-to-introduce-stop-flock-abuse-act-establishing-safeguards-for-ai-powered-cameras/>

³⁶ Network Advertising Initiative, *Advertising Privacy Settings on Mobile Devices*, <https://thenai.org/how-to-opt-out/advertising-privacy-settings-on-mobile-devices/>

³⁷ Network Advertising Initiative, *Advertising Privacy Settings on TVs and Streaming Devices*, <https://thenai.org/how-to-opt-out/advertising-privacy-settings-on-tvs-streaming-devices/>; James K. Willcox, *How to Turn Off Smart TV Snooping Features*, Consumer Reports (October 19, 2025) <https://www.consumerreports.org/electronics/privacy/how-to-turn-off-smart-tv-snooping-features-a4840102036/>

When this app activity data is collected at the app level it can be combined with other consumer data to create detailed profiles of individuals. The Delete Act seeks to address this privacy concern by offering consumers an ability to request that data brokers delete their personal information. Indeed, the Delete Request and Opt-out Platform (DROP) permits Californians to provide their advertising IDs as one of the personal identifiers that data brokers can use to find and delete personal information they have pertaining to the consumer. Unfortunately, due to the different ways that manufacturers approach privacy options regarding this data collection, some consumers may not be able to view this ID in the device settings.³⁸

Requiring that mobile devices, connected TVs, and mobile streaming devices make advertising IDs accessible to consumers would ensure that all consumers can easily find and use this identifier when they make a deletion request in DROP. Additionally, requiring that these devices offer setting options so users can stop this app level tracking and data collection would ensure that all consumers have a way to stop this data collection.

Staff is not aware of previous California legislative proposals targeted to this issue, indicating that it would be a fruitful area to explore. However, in staff's view, further research is needed to develop an effective proposal in this area. Regarding connected TVs in particular, it is difficult to fully assess the problem — or identify effective solutions — given the number of different models and incomplete existing research in this area.

Recommendation: Direct staff to further research this issue and revisit it in 2027. Should bills related to the privacy of connected TVs be introduced this year, staff recommends that the Board consider supporting this or similar legislation.

Require that Connected TV Manufacturers and Operating System Platforms Provide Clear Notice of Automated Content Recognition at Set-up and Require Opt-in Consent

Nearly three-fourths of all homes have a connected TV (CTV) and these devices collect and share large amounts of data.³⁹ Data is collected at the device level, by the manufacturer, operating system provider, or both. This device level collection includes location data, what apps are used and what is watched through antenna or connected apps, manual and voice searches, and often viewing information collected through a technology called automated content recognition (ACR).⁴⁰

ACR is used to collect detailed information about what users view. It is device level technology that collects a small digital fingerprint of what is on the screen and sends that to a server for identification. These fingerprints can be sent as frequently as every minute. The technology can capture what is watched on channels and apps provided by the CTV as well as content consumed via devices connected by HDMI, such as gaming consoles or streaming devices. This granular detail about a consumer's viewing habits can reveal interests, religion, sexuality,

³⁸ James K. Willcox, *How to Turn Off Smart TV Snooping Features*, Consumer Reports (October 19, 2025) <https://www.consumerreports.org/electronics/privacy/how-to-turn-off-smart-tv-snooping-features-a4840102036/>; Network Advertising Initiative, *Advertising Privacy Settings on Mobile Devices*, <https://thenai.org/how-to-opt-out/advertising-privacy-settings-on-mobile-devices/>; Get My IDFA App, available at <https://apps.apple.com/us/app/get-my-idfa/id1580368827>

³⁹ Anselmi, et al, *Watching TV with the Second-Party: A First Look at Automatic Content Recognition Tracking in Smart TVs* (September 10, 2024) <https://arxiv.org/pdf/2409.06203>

⁴⁰ *Id.*; Center for Digital Democracy, *How TV Watches Us: Commercial Surveillance in the Streaming Era* (October 2024) <https://cdn.arstechnica.net/wp-content/uploads/2024/10/CDD-CTV-Report-Oct24-1.1.pdf>

age, and other deeply personal information about the consumer.⁴¹

This viewing information is used to provide personalized content recommendations and shared for targeted advertising. Additionally, the data can be and often is freely sold in the data broker market.

Unfortunately, consumers are often not well informed about this persistent and sensitive data collection or offered a meaningful opportunity to refuse or opt-out of the collection, which has resulted in several legal challenges to the practice under unfair competition law. For example, in 2017 the Federal Trade Commission reached a settlement with Vizio for its surreptitious collection of consumer data by ACR without consumer knowledge or consent.⁴² The settlement required Vizio to disclose its collection practices and get consumer consent before collection and sharing of the viewing data. Similarly, in 2025 the Texas Attorney General brought actions against five TV manufacturers (Sony, Samsung, LG, Hisense, TCL Technology Group Corporation) for ACR data collection.⁴³ Earlier this year Samsung and LG settled and agreed to incorporate clear notices and get informed consent.⁴⁴ The remaining cases are still pending.

Despite the disclosure and consent changes that have occurred as a result of these legal challenges, opting out of ACR is not always easy or without consequence:

- On some CTVs consumers can opt-out of ACR at set-up but refusing the data collection means the consumer is unable to use all the smart TV functionalities. After the FTC settlement, for example, the Vizio TV set up gives consumers a brief notice about ACR and asks them to accept, review full terms, or decline. However, if the consumer declines, most of the functionalities of the smart TV are disabled and they must use a connected device to access apps and channels.⁴⁵ Similarly, on some Roku devices it appears that users have to consent to ACR in order to set up voice commands on the remote.⁴⁶
- There are often multiple levels of data collection that consumers must consider and review. Many CTVs are built with established TV operating system platforms such as Google TV, Amazon Fire TV, and Roku. While Google and Amazon both say that they do not employ ACR in their operating systems to collect viewing data, the TV manufacturer may independently use ACR. As an example, Hisense sells TVs running

⁴¹ Anselmi, et al, *Watching TV with the Second-Party: A First Look at Automatic Content Recognition Tracking in Smart TVs* (September 10, 2024) <https://arxiv.org/pdf/2409.06203>; Federal Trade Commission, *What Vizio was doing behind the TV screen* (February 6, 2017) <https://www.ftc.gov/business-guidance/blog/2017/02/what-vizio-was-doing-behind-tv-screen>

⁴² Federal Trade Commission, *Vizio to Pay \$2.2 Million to FTC, State of NJ to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent* (February 6, 2017) <https://www.ftc.gov/news-events/news/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it-collected-viewing-histories-11-million>

⁴³ Texas Attorney General, *Attorney General Paxton Sues Five Major TV Companies, Including Some with Ties to the CCP, for Spying on Texans* (December 15, 2025) <https://www.texasattorneygeneral.gov/news/releases/attorney-general-paxton-sues-five-major-tv-companies-including-some-ties-ccp-spying-texans>

⁴⁴ Texas Attorney General, *Attorney General Paxton Secures Major Agreement with Samsung to Ensure that Texans are Protected from Smart TVs Collection Their Data Without Their Knowledge* (February 26, 2026) <https://www.texasattorneygeneral.gov/news/releases/attorney-general-paxton-secures-major-agreement-samsung-ensure-texans-are-protected-smart-tvs>; Texas Attorney General, *Attorney General Ken Paxton Secures Major Agreement with LG to Protect Texans' Privacy and Stop Data from Being Collected Without Their Knowledge* (May 11, 2026) <https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-major-agreement-lg-protect-texans-privacy-and-stop-data-being>

⁴⁵ Michael John Wood, *Why Smart TVs Track What You Watch*, Ratings.com (August 5, 2026) <https://www.rtings.com/tv/learn/research/smart-tv-data-privacy>

⁴⁶ *Id.*

the Google TV operating system (OS), Amazon Fire TV OS, Roku OS, and its own VIDAA OS. While the Google TV OS and Amazon Fire TV OS do not use ACR, Hisense TV's themselves appear to utilize this technology and are subject to an ongoing lawsuit brought by the Texas Attorney General.⁴⁷ In practice this means that a user may go through the Google or Amazon Fire TV set-up process, consent or decline various types of data collection that occur at the OS level and still have an additional device-level privacy policy and privacy settings to review or consider.

- Controls can be hard to find and use even when notice is given. While it appears the majority of CTVs have an option in their settings to stop ACR data collection, that control is not always clearly labeled. For example, TCL CTVs give notice of ACR during set-up, but the control a user must access after set-up to deactivate the tool is labeled "Interactive Service." Similarly, Sony CTVs appear to call their ACR control "Samba Interactive TV."⁴⁸ These names are not intuitive or descriptive and therefore may be a blocker for some consumers.

In addition to ACR, CTVs generally collect large amounts of consumer data. For example, the Amazon Fire TV platform does not use ACR, but it does collect information on what you watch through antenna, connected apps, and its own apps as well as what you search for and how you use the platform. Similarly, the Google TV platform also does not use ACR but it collects information on how you use the CTV and combines that with other Google profile data, including what a user may view on YouTube. Many CTVs built with these platforms require users to approve this data collection and create or sign-in with personal accounts to have full smart TV functionalities. Additionally, the settings menus on many of these platforms provide users with varying options to opt-out of certain types of data collection or exercise privacy rights.⁴⁹ However, this industry is so large, with numerous TV manufacturers providing multiple models often built on a variety of operating systems, that it is difficult to have a full accounting of the data collection practices.

The CCPA currently establishes certain requirements that govern data collection by CTVs. Under the law, TV companies and operating systems providers that collect personal information are required to provide notice of what data is collected, how it is used, and whether it is sold or shared. Any additional undisclosed uses of ACR data that are not a business purpose or that fall outside the reasonable expectations of a consumer would require additional consent. Even if a consumer approves ACR data collection, they may still opt out of the sale and sharing of personal information or limit the use and disclosure of any sensitive personal information collected. Additionally, CalPrivacy is currently engaged in pre-rulemaking activities related to notices and disclosure and reducing friction in the exercise of rights that may result in additional regulations that support better notice of these practices and better accessibility of privacy rights.

New requirements to address ACR could further increase consumer awareness of and control over this data collection. For example, the Board could consider:

⁴⁷ James K. Willcox, *How to Turn Off Smart TV Snooping Features*, Consumer Reports (October 19, 2025) <https://www.consumerreports.org/electronics/privacy/how-to-turn-off-smart-tv-snooping-features-a4840102036/>; Michael John Wood, *Why Smart TVs Track What You Watch*, Ratings.com (August 5, 2026) <https://www.rtings.com/tv/learn/research/smart-tv-data-privacy>; Petition for Permanent Injunction, TX v. Hisense USA Corporation, No. C2025-1321D (433rd Judicial District Court, December 15, 2025).

⁴⁸ Michael John Wood, *Why Smart TVs Track What You Watch*, Ratings.com (August 5, 2026) <https://www.rtings.com/tv/learn/research/smart-tv-data-privacy>

⁴⁹ James K. Willcox, *How to Turn Off Smart TV Snooping Features*, Consumer Reports (October 19, 2025) <https://www.consumerreports.org/electronics/privacy/how-to-turn-off-smart-tv-snooping-features-a4840102036/>; Michael John Wood, *Why Smart TVs Track What You Watch*, Ratings.com (August 5, 2026) <https://www.rtings.com/tv/learn/research/smart-tv-data-privacy>

- Requiring CTVs manufacturers to provide improved, clear and conspicuous notice of the collection of viewing data during CTV set-up.
- Requiring that consumers affirmatively consent to ACR data collection or alternatively are easily able to opt-out or disable ACR if additional market research determines that some CTVs do not offer this ability already.
- Whether CTVs may condition full use of smart TV functionality on consent to collection of viewing data.

Clearly, this is an important area that deserves increased attention. In 2015, California adopted AB 1116, which prohibited manufacturers of connected TVs from operating voice recognition features without prominent notice, recording conversations captured by the voice recognition, and selling any conversations for advertising purposes.⁵⁰ A 2022 bill, AB 1262, which would have expanded that law and added an opt-in consent requirement for the sale or sharing of smart speaker transcriptions or recordings, among other things, was vetoed over concerns that if consumers have to opt-in to certain processing in order for the device to work as expected, it would create confusion.⁵¹ Staff is not aware of more recent efforts to control tracking in connected TVs, indicating that it could be a key area to explore. However, given the complexity of data collection ecosystem, the limited and conflicting research in this area, the differences between models, and the complicated interplay between operating systems, apps, and devices, in staff's view, it would require more time to develop an appropriate proposal that would meaningfully advance consumer privacy.

Recommendation: Direct staff to further research this issue and revisit it in 2027. Should bills related to the privacy of connected TVs be introduced this year, staff recommends that the Board consider supporting this or similar legislation.

TIER 3

Continue to Support Re-Introduced Bills Related to Sensitive Personal Information and Publicly Available Information

In 2026, CalPrivacy supported important bills related to sensitive personal information (AB 1542, Ward) and narrowing the publicly available exemption in the CCPA (SB 435, Wahab). Given the importance of these topics, the Legislature may choose to reintroduce these or similar bills. If so, staff would recommend continued support of such bills, subject to Board approval at the appropriate time.

⁵⁰ AB 1116, 2015-16 Leg., Reg. Sess. (Cal. 2015).

⁵¹ AB 1262, 2021-22 Leg., Reg. Sess. (Cal. 2022); Office of the Governor, AB 1262 Veto Message (Sept. 29, 2022), <https://www.gov.ca.gov/wp-content/uploads/2022/09/AB-1262-VETO.pdf?emrc=2fa401>.