SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2021-2022 Regular Session

AB 1262 (Cunningham)
Version: January 3, 2022
Hearing Date: January 12, 2022
Fiscal: Yes
Urgency: No
CK

SUBJECT

Information privacy: other connected device with a voice recognition feature

DIGEST

This bill implements stronger consumer protections in connection with the use of voice recognition features on smart speaker devices and any transcripts or recordings collected or retained in connection with that use.

EXECUTIVE SUMMARY

Existing law prohibits persons or entities from providing the operation of a voice recognition feature associated with connected televisions within this state without prominently informing the user. Recordings or transcriptions collected through the operation of such features for the purpose of improving the voice recognition feature cannot be sold or used for any advertising purpose.

This bill applies these provisions to smart speaker devices and strengthens protections on what can be done with the recordings, and additionally the transcriptions, including limitations on the sharing and retention of the information, as specified. Consumers are required to be properly notified of the features and what activates those features. Companies must receive affirmative consent before sharing or selling transcriptions or recordings, except as provided. Where a speaker retains voice recordings, the user must be provided the opportunity to review and delete those recordings.

This is an author-sponsored bill that is supported by the Children's Advocacy Institute, Oakland Privacy, and Common Sense. It is opposed by various technology and business associations, including the California Chamber of Commerce and TechNet. This bill passed off of the Assembly Floor on a vote of 63 to 0.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Prohibits a person or entity from providing the operation of a voice recognition feature within this state without prominently informing, during the initial setup or installation of a connected television, either the user or the person designated by the user to perform the initial setup or installation of a connected television. (Bus. & Prof. Code § 22948.20(a).)

2) Provides that any actual recordings of spoken word collected through the operation of a voice recognition feature by the manufacturer of a connected television, or a third-party contractor, for the purpose of improving the voice recognition feature, including, but not limited to, the operation of an accessible user interface for people with disabilities, shall not be sold or used for any advertising purpose. (Bus. & Prof. Code § 22948.20(b), (c).)

3) 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).)

4) Provides, pursuant to the California Constitution, that all people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy. (Cal. Const, art. I, § 1.)

5) 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.)

6) States that legally-recognized privacy interests are generally of two classes: interests in precluding the dissemination or misuse of sensitive and confidential information (informational privacy), and interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference (autonomy privacy). (*Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal.4th 1, 35.)

7) 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.)

8) States that no person who owns, controls, operates, or manages a satellite or cable television corporation, or who leases channels on a satellite or cable system shall use any electronic device to record, transmit, or observe any events or listen to, record, or monitor any conversations that take place inside a subscriber's residence workplace, or place of business, without obtaining the express written consent of the subscriber, as specified. (Pen. Code § 637.5(a)(1).)

9) Establishes the California Consumer Privacy Act of 2018 (CCPA), which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. It places attendant obligations on businesses to respect those rights. (Civ. Code § 1798.100 et seq.)

10) Establishes the California Privacy Rights Act (CPRA), which amends the CCPA and creates the Privacy Protection Agency (PPA), which is charged with implementing these privacy laws, promulgating regulations, and carrying out enforcement actions. (Civ. Code § 798.100 et seq.; Proposition 24 (2020).)

11) Provides the following definitions for purposes of the CPRA-amended CCPA:
    a) "consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent.

    b) "deidentified" means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, provided that the business that possesses the information:
        i. takes reasonable measures to ensure that the information cannot be associated with a consumer or household;

ii. publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision; and
iii. contractually obligates any recipients of the information to comply with all provisions of this subdivision.

c) "personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The CCPA provides a nonexclusive series of categories of information deemed to be personal information, including identifiers, biometric information, and geolocation data. (Civ. Code § 1798.140.)

This bill:

1) Defines "smart speaker device" as a speaker and voice command device offered for sale in this state with an integrated virtual assistant connected to a cloud computing storage service that uses hands-free verbal activation.

2) Excludes from the definition above a cellular telephone, tablet, laptop computer with mobile data access, a pager, or a motor vehicle, as defined, or any speaker or device associated with, or connected to, a vehicle.

3) Prohibits a person or entity from providing the operation of a voice recognition feature within this state without prominently informing, during the initial setup or installation of a connected television or smart speaker device, either the user or the person designated by the user to perform the initial setup or installation of the connected television or smart speaker device, that it contains such a feature and what actions or commands activate the feature.

4) Provides that a recording or transcription collected or retained through the operation of a voice recognition feature by the manufacturer of a connected television or smart speaker device, if the recording or transcription qualifies as personal information or is not deidentified, shall not be:

a) used for any advertising purpose;
b) shared with, or sold to, a third party without the user's affirmative consent, except as provided; or
c) retained electronically, unless the user opts in to that retention.

5) Permits a manufacturer to share information with a third party without affirmative consent to the extent sharing that information is necessary to execute

a function or provide a service specifically requested by the user, provided the manufacturer does not use that information for any purpose other than to facilitate the execution of that function or provision of that service.

6) Requires a manufacturer to provide a user with the option to revoke consent for the sharing or sale of data at any time in a manner reasonably accessible to the user. If a user has declined to provide that affirmative consent, the person or entity seeking consent shall not request that affirmative consent for a period of at least one month after the user has declined to provide that affirmative consent, or when the user attempts to access a function that requires affirmative consent.

7) Requires a person or entity that retains voice recordings that qualify as personal information, or are not deidentified, to provide an interface for users to review and delete those recordings. Users must also be given the ability to delete those recordings automatically.

8) Provides that where a person or entity determines that the voice recognition feature was incorrectly activated ("false wake"), the person or entity shall not use the associated audio recording for any purpose, except to improve the accuracy of the voice recognition feature, provided that the user has provided affirmative consent for the use of the audio recording for that purpose.

9) Defines "retained" to mean saving or storing, or both saving and storing, voice recorded data longer than the minimum time necessary to complete a requested command by the user. "Personal information," "deidentified," and "third party" have the same meanings as laid out in the CCPA.

10) Defines "affirmative consent" to mean that a manufacturer of a connected television or smart speaker device has done all of the following:
    a) clearly and conspicuously disclosed to the user, separate from the device terms of use, all of the following to the extent applicable:
        i. the device may be used to process and retain user recordings;
        ii. those recordings may be analyzed or shared with third parties;
        iii. the device may be used to process and retain transcriptions of spoken words; and
        iv. those transcriptions may be analyzed or shared with third parties; and,
    b) clearly and conspicuously disclosed to the user, separate from the device terms of use, the extent to which the device can operate in the absence of consent for each practice described in the above disclosure; and,
    c) received consent, as defined in the CCPA, for each practice described in the above disclosure.

11) Subjects violations of these provisions involving smart speaker devices to the same enforcement scheme as applied to violations involving connected televisions.

COMMENTS

1. Stated intent of the bill

According to the author:

> Existing law (Sections 22948.20, 22948.21, and 22948.23 of the Business and Professions Code) establishes prohibitions for the use of voice recognition features for connected televisions. Today, smart speakers are also equipped with voice recognition features, yet are not included in this section of the B&P code to ensure the same safeguards are in place. This bill would make this section of code more broad, changing the title to include "and Devices," and include smart speaker devices in the provisions.
>
> New safeguards are needed to ensure that consumers can enjoy the benefits of these technologies while mitigating the privacy risks that they pose. Privacy is not a partisan issue and there is a balance that can and needs to be reached—allowing companies to use data to improve their products while ensuring that users' data is not shared or otherwise compromised. There are simply not enough safeguards in place to prevent personal data from being shared. Though Amazon has made some changes, such as allowing someone to say "Alexa, delete everything I've ever said," the burden is still placed on the consumer to ensure their data is removed. Even then, there is not much transparency surrounding how long data is saved, with what third-party applications it is shared before being deleted, et cetera.

2. Protecting the privacy of communications within the home

Conversations within one's home qualify as a type of information protected by established social norms. In *Katz v. United States* (1967) 389 U.S. 347, the U.S. Supreme Court recognized that private conversations in areas secluded from public hearing are protected from government eavesdropping under the Fourth Amendment's search and seizure provisions precisely because there is a societal expectation that such conversations will be afforded a reasonable expectation of privacy. Indeed, California law recognized the protected nature of these communications when it prohibited satellite and cable television corporations from using television equipment to record, listen to, or monitor conversations that take place inside a subscriber's residence without their express written consent. (*See* Pen. Code § 637.5(a)(1).)

Responding to concerns that a new technology, connected televisions, may be recording user conversations without knowledge or consent, AB 1116 (Assembly Privacy and Consumer Protection Committee, Ch. 524, Stats. 2015) was enacted into law. (Bus. & Prof. Code § 22948.20 et seq.) It prohibited the use of voice recognition features without first informing the user about the feature. AB 1116 also prohibited the manufacturer of a connected television and its contractors from selling or using for any advertising purpose actual recordings of spoken word that were collected by the television. It further prohibited a person from compelling another to build specific features into a connected television function that allow investigative or law enforcement officers to monitor communications. AB 1116 authorized the Attorney General or any district attorney to seek a court order enjoining violations of the above prohibitions, as well as seek civil penalties not to exceed $2,500 against those violating this law for each connected television found to violate these prohibitions.

The law further reinforced California residents' right to converse in their homes without fear their conversations will be monitored or recorded by third parties through microphones embedded in their televisions. As technology evolves, so do the collateral consequences to privacy. This bill takes the next step in protecting the conversations taking place in California homes by including smart speaker devices in the framework above.

3. Privacy concerns with the speakers listening to us

The bill defines "smart speaker device" as "a speaker and voice command device offered for sale in this state with an integrated virtual assistant connected to a cloud computing storage service that uses hands-free verbal activation." A smart speaker device does not include "a cellular telephone, tablet, laptop computer with mobile data access, a pager, or a motor vehicle, as defined in Section 415 of the Vehicle Code, or any speaker or device associated with, or connected to, a vehicle."

As an example, one popular such device is Amazon's Echo, which is a smart speaker that uses a cloud-based voice-control system, Alexa, to receive and carry out commands. Alexa software is designed to continuously record snatches of audio, listening for a wake word. When the wake word is detected, the light ring at the top of the Echo turns blue, indicating the device is recording and beaming a command to Amazon servers.

Amazon operates an "Alexa Data Services team" that manages the recordings of human speech and other data that helps train the voice software.[1] The team consists of thousands of employees and contractors across the globe that transcribe, annotate, and

[1] Matt Day, Giles Turner & Natalia Drozdiak, *Amazon's Alexa Team Can Access Users' Home Addresses* (April 24, 2019) Bloomberg, https://www.bloomberg.com/news/articles/2019-04-24/amazon-s-alexa-reviewers-can-access-customers-home-addresses. All internet references are current as of December 28, 2021.

analyze a portion of the voice recordings picked up by Alexa. The program is set up to help Amazon's digital voice assistant get better at understanding and responding to commands. However, troubling reports about the team that listens to recordings of what goes on in the homes of millions of users raises serious privacy concerns not unlike the ones addressed by the laws discussed above.

The Alexa team is essentially listening in on the private conversations going on in the many households that use these smart speakers. Members of the team themselves worried that the company was "granting unnecessarily broad access to customer data that would make it easy to identify a device's owner." A Bloomberg investigation found that Amazon employees and contractors were able to use location data to identify the home addresses of the households they were listening to recordings of.

The team has a chat mechanism they can use to share recordings they find amusing and some that are disturbing:

> Sometimes they hear recordings they find upsetting, or possibly criminal. Two of the workers said they picked up what they believe was a sexual assault. When something like that happens, they may share the experience in the internal chat room as a way of relieving stress. Amazon says it has procedures in place for workers to follow when they hear something distressing, but two Romania-based employees said that, after requesting guidance for such cases, they were told it wasn't Amazon's job to interfere.[2]

In addition to the live persons listening to the recordings, the policies regarding retention of the recordings has also drawn scrutiny.

> Your Amazon Echo speaker is listening to you, but it also remembers what you said. CNET discovered that the Alexa digital assistant keeps a record of your voice transcriptions and even shares them, with no expiration date in sight. The text transcripts stay stored on Amazon's servers until you delete the voice recordings. Amazon is **still working on removing the data from all parts of its systems when you delete your transcripts**. It's unclear when that will happen.
>
> The company asserts that the data is used to improve Amazon Echo. That's not uncommon. Apple stores anonymized Siri data for up to two years in order to improve the product. Amazon's reason is likely the same,

[2] Matt Day, Giles Turner & Natalia Drozdiak, *Amazon Workers Are Listening to What You Tell Alexa* (April 10, 2019) Bloomberg, https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio (emphasis added).

> using your data -- and everyone else's -- to improve the way Echo understands you.
>
> However, with past slip-ups that included Alexa sending a private family conversation to a random contact, you may feel a bit uneasy about Amazon keeping your recorded commands.
>
> "When a customer deletes a voice recording, we delete the transcripts associated with the customer's account of both of the customer's request and Alexa's response," Amazon said in a statement. "We already delete those transcripts from all of Alexa's primary storage systems, and we have an ongoing effort to ensure those transcripts do not remain in any of Alexa's other storage systems."[3]

United States Senator Chris Coons sent a letter to Amazon CEO Jeff Bezos seeking clarity on the operation and processes involved with the Alexa system and specifically how long it kept voice recordings and transcripts, and what the data gets used for.[4] The letter was sent in the wake of reports that Amazon kept transcripts of interactions with Alexa, even after people deleted the voice recordings.

In its response, the company made clear that Amazon keeps transcripts and voice recordings indefinitely, and only removes them if they are manually deleted by users. It further noted that Amazon had an "ongoing effort to ensure those transcripts do not remain in any of Alexa's other storage systems." Nevertheless, there are still records from some conversations with Alexa that are not deleted, even if people remove the audio, the letter revealed. The Senator responded:

> "Amazon's response leaves open the possibility that transcripts of user voice interactions with Alexa are not deleted from all of Amazon's servers, even after a user has deleted a recording of [their] voice," the lawmaker said in a statement. "What's more, the extent to which this data is shared with third parties, and how those third parties use and control that information, is still unclear."

4. Expanding the law to cover this new technology

This bill attempts to put up privacy guardrails around these devices and their voice recognition features. It requires a person or entity seeking to provide the operation of a voice recognition feature to first prominently inform the user that the device contains

---

[3] Sharon Profis & Rick Broida, *You can finally delete (most of) your Amazon Echo transcripts. Here's how* (July 3, 2019) cnet, https://www.cnet.com/how-to/you-can-finally-delete-most-of-your-amazon-echo-transcripts-heres-how/.

[4] Alfred Ng, *Amazon Alexa keeps your data with no expiration date, and shares it too* (July 2, 2019) cnet, https://www.cnet.com/news/amazon-alexa-keeps-your-data-with-no-expiration-date-and-shares-it-too/.

such a feature, as well as what actions or commands will activate the feature to record or transcribe audio. These disclosures are a common sense transparency measure to ensure that consumers know that the smart speaker device they have is equipped with such a feature and its basic operation.

The bill also provides limitations on what can be done with recordings or transcriptions collected or retained through a voice recognition feature. If the recording or transcription is personal information, and is not deidentified, as those terms are defined in the CCPA, it cannot be used for any advertising purpose and users must first provide affirmative consent before it can be shared with, or sold to, any third party. This ensures that this sensitive information, which can reasonably identify, relate to, describe, be capable of being associated with, or be linked to a particular consumer, is not being used for the commercial purposes of the person collecting your information.

Where a user provides affirmative consent for the sharing or sale of their data, the bill requires the manufacturer to provide users with the ability to revoke that consent at any time. This allows the user to be more in control of their device and their information. In order to avoid a constant barrage of requests for consent, the bill places a waiting period after a user declines to provide consent before the person or entity seeking consent can again request it. A previous version placed this timeline at 12 months.

Amazon expressed concerns that this provision placed "an unnecessary and arbitrary restriction on a company's ability to inform its customers about the utility of their device and how it may be impacted by their privacy choices." In response, the author has recently taken amendments to the bill and shortened this period to one month. In addition, the person or entity can again seek consent for the sharing or sale of data "when the user attempts to access a function that requires affirmative consent." This ensures that functionality is not unknowingly impaired by a user's decision not to consent. Again, this places the user in control, but ensures they are making an informed decision.

To address concerns expressed by opposition that this hinders some of the basic functions of the device through which users intend their information to be used, the bill provides an exception by which information may be shared with a third party without affirmative consent "to the extent sharing that information is necessary to execute a function or provide a service specifically requested by the user." For example, if a user asks the speaker to order a pizza, the device does not need to secure affirmative consent to share the order with the pizzeria. Amazon raised concerns with a previous provision that only allowed this functionality if the *third party* did not use the information for any other purpose. As the manufacturer is not best situated to control third parties, the author has amended this provision to allow the manufacturer to only use that information to facilitate the execution of the requested function or provision of that service.

The bill also requires a user to opt in to a manufacturer retaining recordings electronically. It should be noted that data is not "retained" if kept solely for the time period necessary to complete a requested command by the user. If recordings are retained, users must be provided an interface to review and delete those recordings. This is a feature that already exists for at least some smart speaker devices, and keeps the user in the driver seat. The user's rights with respect to these recordings must be clearly communicated to the user.[5] The bill also requires users be given the ability to delete such recordings automatically.

The bill also deals with so-called "false wakes," where a smart speaker device activates inadvertently and not in response to designated "wake words," such as "Hey, Siri." As users likely do not anticipate that such recordings will be kept and used for other purposes, the bill prohibits the use of audio recordings associated with these improper wakes for any purpose, with one exception. Amazon and others have indicated that they use these inadvertent recordings to improve the accuracy of the voice recognition features. The bill permits the recordings to be used for these purposes so long as users consent to such use.

The bill makes clear that manufacturers are not liable for functionality provided by applications that the user chooses to use in the cloud or that are downloaded and installed by a user, unless the manufacturer collects, controls, or has access to any personal information collected or elicited by the applications.

5. Ensuring meaningful consent

The bill bases its definition of consent on the recent language adopted through Proposition 24, amending the CCPA. The language ensures that consent is freely given and is not obtained through confusing or misleading methods, such as through the use of dark patterns.

"Affirmative consent" also requires that the manufacturer has clearly and conspicuously disclosed specific information to the user, as applicable. This includes notifying the user if the device may be used to process and retain user recordings; if those recordings may be analyzed or shared with third parties; and if the device may be used to process and retain transcriptions of spoken words and if those transcriptions might be analyzed or shared with third parties. There must also be a clear disclosure, separate from the device terms of use, explaining the extent to which the device can operate in the absence of consent for each of these practices.

[5] Amazon raised concerns with a previous version of the bill that simply referenced a "user's rights." Recent amendments make clear that the relevant rights are those provided pursuant to the chapter of the Business and Professions Code being amended by this bill.

6. Stakeholder positions

Writing in support, Common Sense asserts the bill "gives consumers the ability to ensure, if they wish, that what they say in their homes stays in their homes, and isn't mined by corporations." It states:

> As privacy and consumer advocates, we write to express our SUPPORT of AB 1262. As you well know consumers are especially concerned about invasive connected devices that sit in cars, kitchens, family rooms, and bedrooms. Indeed, a recent survey on smart speakers and voice assistants conducted by Common Sense Media found that more than nine in ten parents of young kids say that it is important to them that they can control the information collected about their family. Families want control, but one third of those surveyed said that while they would like to limit the information collected by such devices, they did not know how.
>
> We appreciate that this bill gives consumers more control over the information collected about them in intimate spaces such as their homes.

The coalition in opposition, including TechNet, the Civil Justice Association of California, and the Consumer Technology Association, which represent Amazon, Google, and Facebook, along with other companies, asserts:

> AB 1262 prohibits the use of data collected from "incorrect activations" for any purpose other than to improve the device. AB 1262 requires a user to opt-in before a business can use an audio recording associated with an incorrect activation to improve the accuracy of the device. As a threshold issue, businesses cannot know whether the information was captured through incorrect activation until it is analyzed and determined as such. §22948.20(g)(1) states that a person or entity providing the operation of a voice recognition feature "determines that the voice recognition feature was incorrectly activated," the person or entity shall not use the associated audio for any purpose except as provided in section §22948.20(g)(2). Implicit in this logic is that one does not know whether the information was captured through incorrect activation until it is analyzed, which takes time. Accordingly, in-order to operationalize this section, it is important that a business be permitted to retain data for a reasonable period of time in order to determine if it is the result of incorrect activation. Further, the only way to improve the accuracy of voice recognition devices and prevent future incorrect activation is to allow the use of this information to help improve device functionality. Analysis of this data is also important for improving functionality for people with different speech patterns, including people who suffer from ailments that affect their speech. Requiring consumers to opt-in to business use of data to improve

> their own products and services will thus increase user frustration and slow down the ability to improve these devices.

Another concern that was highlighted by various technology associations and companies, including those officially in opposition, was the rigid prohibition on using recordings or transcriptions for advertising purposes. The coalition argues:

> AB 1262 bans the use of this information for advertising, regardless of consumer choice. AB 1262 as drafted prohibits the use of information collected through smart speakers for any and all advertising purposes, including first party advertising, regardless of consent. The bill effectively revokes a person's existing freedom to make that choice for herself. (§22948.30(b)(1)). We respectfully urge reconsideration of this outright ban on any use of this information for advertising.

In response to this concern, the author has agreed to an amendment that allows for recordings or transcriptions collected from smart speaker devices to be used for advertising purposes if the user has provided affirmative consent to such use.

SUPPORT

Children's Advocacy Institute
Common Sense
Oakland Privacy

OPPOSITION

American Association of Advertising Agencies
Association of National Advertisers
Billion Strong
California Chamber of Commerce
Civil Justice Association of California
Consumer Technology Association
Entertainment Software Association
Interactive Advertising Bureau
Internet Association
Ruh Global Impact
TechNet

RELATED LEGISLATION

Pending Legislation:

SB 210 (Wiener, 2021) provides greater transparency and accountability with respect to automated license plate recognition (ALPR) systems. It requires ALPR operators and end-users to conduct annual audits to review ALPR searches. If the operator or end-user is a public agency, the bill further requires them to destroy all ALPR data that does not match information on a hot list within 24 hours. This bill was held in the Senate Appropriations Committee.

SB 346 (Wieckowski, 2021) requires the disclosure of in-vehicle cameras installed by the manufacturer and places restrictions on what can be done with video recordings from such cameras and where such recordings can be retained. The bill prohibits compelling an entity to build specific features for the purpose of allowing the monitoring of communications. This bill is currently in the Assembly Privacy and Consumer Protection Committee.

Prior Legislation:

AB 1395 (Cunningham, 2020) was nearly identical to the previous version of this bill. It died in the Senate Judiciary Committee.

AB 1215 (Ting, Ch. 579, Stats. 2019) prohibits law enforcement from installing, activating, or using a biometric surveillance system in connection with a law enforcement agency's body-worn camera or any other camera worn or carried.

SB 327 (Jackson, Ch. 886, Stats. 2018) requires manufacturers of connected devices to equip those devices with reasonable security features appropriate to the nature of the device.

AB 1116 (Assembly Committee on Privacy and Consumer Protection, Ch. 524, Stats. 2015) *See* Comment 2.

PRIOR VOTES:

Assembly Floor (Ayes 63, Noes 0)
Assembly Appropriations Committee (Ayes 16, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 10, Noes 0)

****