Date of Hearing: April 22, 2021

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 1262 (Cunningham) – As Introduced February 19, 2021

SUBJECT: Information privacy: other connected device with a voice recognition feature

SUMMARY: This bill would establish limitations on the use, retention, sharing, and sale of recordings or transcriptions containing personal information (PI) collected by the voice recognition feature of a smart speaker device, and would prohibit a person or entity from providing the operation of a voice recognition feature without prominently informing the user during initial setup of a smart speaker device. Specifically, **this bill would**:

1) Prohibit 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 smart speaker device, either the user or the person designated by the user to perform its initial setup or installation.

2) Provide that a recording or transcription collected or retained through the operation of a voice recognition feature by the manufacturer of a smart speaker device, if the recording or transcription qualifies as PI or is not deidentified, shall not be: (1) used for any advertising purpose; (2) shared with, or sold to, a third party, unless the user has provided affirmative written consent, as defined; or (3) retained electronically, unless the user opts in to having that recording retained by the manufacturer either during installation or at a later time in the device settings.

3) Specify that a manufacturer may be held liable for functionality provided by applications that the user chooses to use in the cloud or are downloaded and installed by a user if the manufacturer collects, controls, or has access to any PI collected or elicited by the applications.

4) Exclude from these requirements devices used only to record medical or research information, as specified.

5) Make conforming changes to parallel statutes to the extent they currently apply to connected televisions.

6) Define "affirmative written consent" to mean a manufacturer of a connected television or smart speaker device provided the following disclosure to a user during installation of a device, separate from the device terms of use, and received authorization from the user pursuant to the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.) and the Uniform Electronic Transactions Act (Title 2.5 (commencing with Section 1633.1) of Part 2 of Division 3 of the Civil Code):

> "*This device may be used to process and retain user recordings and transcriptions of spoken words. Those recordings may be analyzed and shared with third parties by the manufacturer and its employees for the purpose of improving the device. Please indicate whether or not you give your consent for the device to be used in this way. This consent is not required to use basic functions of this device.*

I authorize [manufacturer name] to share my recordings, and I understand that the recordings may be analyzed and shared with third parties by the manufacturer and its employees.

I do not authorize [manufacturer name] to share my recordings and I do not want to have access to the enhanced smart features of this device."

7) Define "smart speaker device" to mean 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; and would specifically exclude from this definition a cellular telephone, a tablet, a laptop computer with mobile data access, a pager, or a motor vehicle, or any speaker or device associated with, or connected to, a vehicle.

8) Define the following terms for the purposes of these provisions: cloud computing storage service; deidentified; personal information; retained; third party; user; and voice recorded data.

EXISTING LAW:

1) Bans, under the federal Electronic Communications Privacy Act of 1986, the interception of electronic communications, such as email, radio-paging devices, cell phones, private communications carriers, and computer transmissions. (18 U.S.C. Secs. 2510-2522, 2701-2711, 3121, and 1367.)

2) Provides that, among other rights, all people have an inalienable right to pursue and obtain privacy. (Cal. Const., art., Sec. 1.)

3) Prohibits, with exceptions, electronic eavesdropping or recording of private communications by telephone, radio telephone, cellular radio telephone, cable or any other device or in any other manner. Violation can result in penalties of up to $10,000 and imprisonment in county jail or state prison for up to one year. (Pen. Code Secs. 630-638.)

4) Prohibits cable and satellite television operators from monitoring or recording conversations in a subscriber's residence, except as specified, or from sharing individually identifiable information on subscriber viewing habits or other personal information without written consent. (Pen. Code Sec. 637.5.)

5) Governs connected televisions to prohibit any 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 the connected television. (Bus. & Prof. Code Sec. 22948.20(a).)

6) Prohibits actual recordings of spoken word collected through the operation of a voice recognition feature by the manufacturer of a connected television, or by a third party contracting with a manufacturer, 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, from being sold or used for any advertising purpose. (Bus. & Prof. Code Sec. 22948.20(b).)

7) Prohibits any 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 Sec. 22948.20(c).)

8) Specifies that a manufacturer shall only be liable for functionality provided at the time of the original sale of a connected television and shall not be liable for functionality provided by applications that the user chooses to use in the cloud or that are downloaded and installed by a user. (Bus. & Prof. Code Sec. 22948.20(d).)

9) Gives the Attorney General or a district attorney the power to prosecute a manufacturer that violates or proposes to violate these provisions by seeking injunctive relief, a civil penalty of up to $2,500 per violation, or both, and are cumulative. (Bus. & Prof. Code Sec. 22948.23(c).) Specifies that there is no private right of action for violation of these provisions, nor do these provisions limit any existing right of private action. (Bus. & Prof. Code Sec. 22948.23(a).)

10) Defines "connected television" for these purposes to mean a video device designed for home use to receive television signals and reproduce them on an integrated, physical screen display that exceeds 12 inches, except that this term shall not include a personal computer, portable device, or a separate device that connects physically or wirelessly to a television, including, but not limited to, a set-top box, video game console, or digital video recorder. (Bus. & Prof. Code Sec. 22948.21(a).)

11) Defines "voice recognition feature" for these purposes to mean the function of a connected television that allows the collection, recording, storage, analysis, transmission, interpretation, or other use of spoken words or other sounds, except that this term shall not include voice commands that are not recorded or transmitted beyond the connected television. (Bus. & Prof. Code Sec. 22948.21(c).)

12) Establishes the California Consumer Privacy Act of 2018 (CCPA) to provide various rights to consumers. Subject to various general exemptions, the CCPA grants a consumer, among other things: (1) the right to know what PI is collected and sold about them; (2) the right to request access to the specific PI the business has retained about them; (3) the right to request the deletion of the PI that the business has collected about them; (4) the right to opt-out of the sale of their PI, or opt-in in the case of minors under 16 years of age; and (5) the right to pursue a cause of action against a business that has suffered a data breach in the event the consumer's PI has been impermissibly accessed. (Civ. Code Sec. 1798.100 et seq.)

13) Prohibits a business from discriminating against a consumer because the consumer exercised any rights under the CCPA, including, but not limited to, by: denying goods or services to the consumer; charging different prices or rates for goods or services; providing a different level or quality of goods or services to the consumer; or suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services. (Civ. Code Sec. 1798.125(a)(1).)

14) Specifies that the prohibition in 14), above, does not prohibit a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or

services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data. (Civ. Code Sec. 1798.125(a)(2).)

15) Defines "deidentified," for the purposes of the CCPA, to mean information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information: (1) has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain; (2) has implemented business processes that specifically prohibit reidentification of the information; (3) has implemented business processes to prevent inadvertent release of deidentified information; and (4) makes no attempt to reidentify the information.

16) Defines "personal information," for the purposes of the CCPA, to mean 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, including, but not limited to, biometric information and audio, electronic, or similar information, among others. (Civ. Code Sec. 1798.140(o).) CCPA also defines "biometric information" to include voice recordings from which an identifier template such as a voiceprint can be extracted. (Civ. Code Sec. 1798.140(b).)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of this bill**: This bill seeks to expand protections for consumers' PI by establishing specific limitations on the use, retention, sharing, and sale of recordings or transcriptions collected by the voice recognition feature of a smart speaker device. This bill is author sponsored.

2) **Author's statement**: 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.

3) **Smart speakers and the right to privacy in the home**: In 1967, the United States Supreme Court held that private conversations secluded from public protected against government surveillance under the Fourth Amendment's protections against unreasonable search and seizure. (*Katz v. United States* (1967) 389 U.S. 347.) The decision in that case relied heavily on affirming the existence of a reasonable societal expectation that private conversations in areas secluded from the public will be afforded privacy. Since then, the proliferation of so-called "smart" devices, with the ability to both actively and passively collect various types of information, have redefined our understanding of this expectation.

   The role of smart devices in the daily lives of Americans has skyrocketed in recent years with the emergence of smart technologies designed to increase personal comfort, convenience, and efficiency. These devices are varied in nature, and include Wi-Fi enabled speakers, thermostats, door locks, cameras, lights, security systems, sprinklers, and refrigerators. According to a 2017 report by McKinsey, 29 million homes in the United States had some form of smart technology, and this number has been growing at an average rate of 31% per year.[1]

   Given this rate of growth, it is reasonable to expect that the diversity of smart technology in homes will only increase over time, and as a result, the pervasiveness of connected devices with the capacity to affect lives in the home, vehicle, and otherwise is also likely to increase. Considering the ability of these devices to collect information that can be retained, and some cases shared or sold, by the manufacturer of the device, however, raise questions as to how we define our reasonable expectation of privacy in the home, and whether specific safeguards are necessary to ensure that smart devices preserve that expectation.

   In an alarming exposé published in 2019, *Bloomberg* revealed the extent to which employees of Amazon have access to the recordings made by consumers' Amazon Echo smart speakers, which utilize a cloud-based virtual assistant reliant on voice recognition called "Alexa".[2] These devices regularly record small snippets of audio in order to listen for a wake word that activates the virtual assistant, and, when activated, the ensuing commands are then transmitted to the "Alexa Data Services Team," who are responsible for transcribing, annotating, and analyzing some of these voice recordings to improve the device's voice recognition and language processing functions. As the *Bloomberg* report indicates, however, the team responsible for managing this data are often exposed to deeply personal conversations and occurrences that could easily be associated with individuals. Members of the Alexa Data Services Team, according to the article, voiced concerns that they were granted "unnecessarily broad access to customer data that would make it easy to identify a device's owner." The article describes:

   > Occasionally the listeners pick up things Echo owners likely would rather stay private: a woman singing badly off key in the shower, say, or a child screaming for help. The teams use internal chat rooms to share files when they need help parsing a muddled word – or come across an amusing recording.

---

[1] K. Ahuja & M. Patel, "There's No Place Like [A Connected] Home", *McKinsey & Company*, 2017.
[2] M. Day, G. Turner, & N. Drozdiak, "Amazon Workers Are Listening to What You Tell Alexa", *Bloomberg*, Apr. 10, 2019, https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio, [as of Apr. 17, 2021].

> 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.[2]

Studies show that a significant portion of consumers are concerned as to how smart speakers may affect their personal privacy. As Oakland Privacy describe in support of the bill:

> Consumers want the protections provided by AB 1262. A 2020 marketing poll from Hub Entertainment Research found 91 per cent of smart speaker users said they are worried about unwanted listening by their speakers, and 90 per cent of owners said they are concerned about data being unknowingly collected. And two-thirds (66 per cent) of consumers who are yet to buy a smart speaker admit that privacy is a main reason why they haven't purchased one. [Citation] While we don't yet know how much industry opposition [to this] bill may exist, these polls indicate that the growth of the market for these devices is intrinsically connected to the degree of confidence consumers have regarding their ability to protect themselves from privacy risks.
>
> Consumers are right to worry. Digital security websites are full of warnings and advice on security issues with smart speakers. An internationally publicized report from Check Point found in August 2020 that gaining access to voice records of an Alexa device was a one click hack. [Citation] A year earlier, researchers from Talos issued a similar warning for Google's Nest devices. [Citation]

However, the relationship between these devices and personal privacy is not necessarily as straightforward as one might expect. As Ruh Global IMPACT and Billion Strong point out in opposition to this bill:

> Smart speakers have eliminated barriers and provided independence for the millions of us living with disabilities. They have empowered us to perform tasks otherwise provided by a caregiver, such as calling others for assistance, adjusting the temperature in our homes, shopping online, locking and unlocking doors to receive deliveries, setting security alarms, turning lights on and off, and raising and lowering blinds.
>
> We value our privacy as much as anyone – and support well-informed privacy protections for smart speaker devices. However, as smart devices enable us to live independently in our own homes – this reduces our reliance on family, friends, and caregivers to perform basic tasks – given this, smart speakers truly create privacy for us.

This bill seeks to provide protections for the particularly sensitive data than can be recorded by smart speakers without eliminating their utility.

4) **Rights regarding smart speaker data under CCPA**: A coalition of business advocacy groups in opposition to this bill detail several actions this Legislature has already taken to protect smart speaker data through general protections for personal information:

> In 2018, California passed two landmark measures regulating internet-connected devices, effective January 1, 2020. First, the California Consumer Privacy Act (CCPA) of 2018, AB 375 (Chau, Hertzberg, Dodd), provides consumers with the right to access, delete, and opt-out of sale of their personal information – including voice recognition data.

Second, in 2020, California voters approved the California Privacy Rights Act, which further expanded the rights of the CCPA, adding the right to correct, limiting the use of sensitive personal information, expanding opt out rights to include cross-contextual behavioral advertising, and much more. . Third, the legislature passed an Internet of Things (IoT) measure, AB 1906 (Irwin)/SB 327 (Jackson), which requires that all internet-connected devices – including devices with voice recognition features - contain reasonable security features for the device and the information the devices collect, contain, and transmit. These laws are comprehensive and cover devices with voice recognition features in a technology neutral manner.

The CCPA (AB 375, Chau, Ch. 55, Stats. 2018), in particular, gives consumers certain rights regarding their personal PI, such as: (1) the right to know what PI is collected and sold about them; (2) the right to request access to the specific PI the business has retained about them; (3) the right to request the deletion of the PI that the business has collected about them; (4) the right to opt-out of the sale of their PI, or opt-in in the case of minors under 16 years of age; and (5) the right to pursue a cause of action against a business that has suffered a data breach in the event the consumer's PI has been impermissibly accessed.

In the context of smart speaker devices, the CCPA affords the consumer the ability to opt-out of the sale or disclosure of their information by smart speaker devices to others and ensures that the business would have to honor that request upon receipt of a verifiable consumer request, as specified. The consumer could also ask the business to delete their PI collected from the device, and the business would not only have to delete the information but instruct any service providers[3] to delete the consumer's PI from their records as well. In either scenario, a business could not suddenly retaliate or seek to coerce a consumer to opt back in by disabling the device altogether, as storing or selling the information is not likely reasonably necessary in terms of the functionality of the device itself. Of course, under the CCPA, with respect to the right of deletion, there are some limitations to the right to delete, insofar as it is necessary for the business or service provider to maintain the PI in order to carry out various activities. These include where it is necessary to:

- Complete the transaction for which the PI was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or to otherwise perform a contract between the business and the consumer.

- Debug to identify and repair errors that impair existing intended functionality.

- Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business. (Civ. Code Sec. 1798.105.)

There is nothing in the CCPA specific to smart speakers to give consumers the option of opting-in and or out of these devices collecting voice recording or passively eavesdropping

[3] Under the CCPA, service providers, in contrast to third party businesses, are those entities that provide necessary services to the business to perform the services requested by the consumer, assuming that the consumer has received notice from the business that information is being used or shared in the business's terms and conditions, as specified, and the service provider does not use the PI for any purposes other than assisting the business.

on private conversations, but the CCPA does provide for the ability of consumers to opt-out of the sale of their PI, or delete their PI, without naming any technologies or specific businesses. As long as a business is subject to the CCPA (*i.e.*, meets one of the thresholds that would cause the business to fall within the CCPA's definition of "business"), they would have to comply with the data privacy law, subject to certain exemptions.

5) **AB 1116 (Com. on P&CP, Ch. 524, Stats. 2015) and smart televisions**: In 2015, this Committee authored a bill that generally prohibited the collection and use of spoken words and conversations captured by internet-connected televisions, commonly known as "connected televisions" or "smart TVs," without first prominently informing either the user or the person designated by the user to initially set up or install the television, during the initial setup or installation of the television.

   That bill, AB 1116 (Committee on Privacy and Consumer Protection, Ch. 524, Stats. 2015), further prohibited the use or sale for advertising purposes any spoken words or sounds collected through a connected television for purposes of improving the voice recognition feature. AB 1116 also prohibited the collection of actual recordings of spoken words through the operation of a voice recognition feature for the purposes of improving the voice recognition feature from being sold or used for any advertising purpose. These rights are subject to enforcement by the Attorney General or a district attorney. The law does not expand or limit any other existing private rights of action that may reside at law for the consumer.

   For these purposes, the connected television law, as enacted by AB 1116, defines "connected television" to mean a video device designed for home use to receive television signals and reproduce them on an integrated, physical screen display that exceeds 12 inches, except that this term shall not include a personal computer, portable device, or a separate device that connects physically or wirelessly to a television, including, but not limited to, a set-top box, video game console, or digital video recorder. The law defines "voice recognition feature" to mean the function of a connected television that allows the collection, recording, storage, analysis, transmission, interpretation, or other use of spoken words or other sounds, except that this term shall not include voice commands that are not recorded or transmitted beyond the connected television. (Bus. & Prof. Code Sec. 22948.21.)

   This bill seeks to address a very similar issue, in how smart speaker devices, such as the Amazon Alexa or Google Home, can similarly listen for and respond to consumer commands.

6) **AB 1395 (Cunningham, 2019) sought to regulate certain data collected by smart speakers**: In 2019, the author of this bill introduced AB 1395, which sought to expand upon the CCPA's general protections in the specific context of smart speakers. AB 1395, as it was introduced, would have provided that a smart speaker device, or a smart speaker device manufacturer, as respectively defined, shall not save or store recordings of verbal commands or requests given to the smart speaker device, or verbal conversations heard by the smart speaker device, regardless of whether the smart speaker device was triggered using a key term or phrase. It also would have defined "smart speaker device" to mean "a wireless speaker and voice command device sold in this state with an integrated virtual assistant that offers interactive actions and hands-free activation," but explicitly excluded from the definition "a cell phone, tablet, or laptop computer with mobile data access, or a pager."

Noting the similarity between the objectives of AB 1395 and AB 1116, this Committee's analysis of that bill recommended that rather than establishing a separate law, the bill should instead amend the connected television statutes to include this particular type of voice recognition feature, among others. As the analysis noted:

> Arguably, this bill should, instead, of establishing a separate law, amend the connected television statutes to instead apply more generally to connected devices with voice recognition features. To this end, it is unclear why this bill currently applies to any wireless speaker and voice command device sold in this state with an integrated virtual assistant that offers interactive actions and hands-free activation, while also excluding from the bill any cellular telephone, tablet, or laptop computer with mobile data access, or a pager – even though many cellphones and tablets today share the same types of voice recognition features that rely on voice commands or prompts from the user. If this Committee were to approve this bill, it may wish […] to strike the provisions of the bill and expand the connected television statutes to capture any such connected device equipped with a voice recognition feature, as suggested below. Such a term would include a wireless speaker and voice command device sold in this state with an integrated virtual assistant that offers interactive actions and hands-free activation, as well as a cellular telephone, tablet, or other device sold in this state with an integrated virtual assistant that offers interactive actions and hands-free activation.

In accordance with that suggestion, the author of the bill initially amended AB 1395 to expand the smart television statute established by AB 1116 to include "other connected device[s] with a voice recognition feature," and made other substantive adjustments to that law, including: amending the applicability of its protections to "a recording or transcription collected or retained through the operation of a voice recognition feature […] if that recording or transcription qualifies as personal information or is not deidentified" as defined in the CCPA, rather than to "any actual recordings or transcripts collected […] for the purpose of improving the voice recognition feature"; and prohibiting the use of such data for any advertising purpose outright, rather than permitting a user to affirmatively consent to that use. The bill passed out of this Committee with no "no" votes.

Ultimately, however, AB 1395 was pared back to include only smart speakers, and to explicitly exclude "a cellular telephone, a tablet, a laptop computer with mobile data access, a pager, or a motor vehicle […] or any device associated with, or connected to, a vehicle." AB 1395 died in the Senate Judiciary Committee without receiving a hearing, in part due to constraints on the legislative process imposed by the COVID-19 pandemic.

7) **AB 1262 reintroduces the final version of AB 1395, including its limitation to smart speakers**: AB 1262, as it is in print, is identical to AB 1395 as it died in Senate Judiciary Committee. Specifically, the bill would amend the smart television statute established by AB 1116 to include a "smart speaker device," and would apply the core protections of the bill to recordings or transcripts collected or retained through the operation of a voice recognition feature of these devices so long as the recording or transcription qualifies as personal information or is not deidentified, whether or not the information was collected "for the purpose of improving the voice recognition feature." The bill would also prohibit the use of such information for any advertising purposes, and would not provide the user the ability to opt-in to such uses, in contrast to the sale, sharing, and electronic retention of the information that are permitted only if the consumer provides affirmative consent. Additionally, the bill

would expand manufacturer liability relative to the existing law, which currently exists only with respect to the functionality provided at the time of the original sale of a connected television, to include functionality provided by applications that the user chooses to use in the cloud or are downloaded and installed by the user if the manufacturer collects, controls, or has access to any personal information collected or elicited by the applications. Finally, the bill prescribes very specific language that must be used to obtain affirmative written consent for the purposes of the bill, and defines several relevant terms.

Staff notes that whether, on balance, amending the connected television, and proposed smart speaker, statute to apply to "a recording or transcription collected or retained through the operation of a voice recognition feature […] *if the recording or transcription qualifies as personal information or is not deidentified*" as opposed to "any actual recordings of spoken word collected through the operation of a voice recognition feature […] *for the purpose of improving the voice recognition feature*" would broaden or narrow its applicability requires careful consideration. The changes to the existing connected television law proposed by this bill would remove the requirement that the recordings be of spoken word, and that the recordings be collected for the purpose of improving the voice recognition feature, but also limits its application to personal information that is not deidentified.

Both "personal information" and "deidentified" have the same meaning as in the CCPA as in this bill. Under the CCPA, PI is defined to mean "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," and specifically includes biometric information; internet or other electronic network activity including browsing history, search history, or information regarding a consumer's interaction with a website, application, or advertisement; and audio, electronic, or similar information, among others; so long as that information identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked with a particular consumer or household. (Civ. Code Sec. 1798.140(o).) Most likely, voice recordings of individuals would be considered PI under this definition, since CCPA also defines "biometric information" to include "voice recordings from which an identifier template such as […] a voiceprint can be extracted." (Civ. Code Sec. 1798.140(b).) Because audio recordings are also considered PI under the CCPA if they can reasonably be linked to a particular consumer or household, it would seem this change in applicability would generally expand the breadth of information to which the protections of the bill apply, since it would include both "spoken word" and other recordings that could in some way be linked to the person. Taking into consideration that the existing language also limits the statutory protections based on the intent of collection, i.e., to information recorded for the purpose of improving the voice recognition feature, this change to the statute created by AB 1116 seemingly improves the ability of these protections to capture a wide range of putatively personal recordings a smart speaker may collect.

Regarding the protections the bill provides, Oakland Privacy adds in support of the bill:

> These are appropriate protections for conversations never intended for any outside or public use and which are part of what is legally and ethically considered the personal domain; what we say in our own home to the people we live with and whom we invite into our homes. While they can be convenient, the ubiquity of smart speaker devices mean that despite a consumer's best intentions, it is more likely than not that they will

> often forget to turn the device "off" during times of intimate conversation or personal crisis. A requirement that they do so if they don't want manufacturer employees listening to their fights, to the sound of them crying, to their evening rituals or to a difficult phone call is patently unreasonable. Our home is our home for the precise reason that we do not have to worry about a eavesdropper as we do when out in a public space.
>
> The bill is not prescriptive. For those consumers who feel they can exercise sufficient control over their device usage to protect themselves, and whose interest in improving the responsiveness of the device's voice recognition features supersedes their privacy concerns, they can clearly consent to helping to train the devices. But for those with complex living situations, or who are inclined to forgetfulness, an explicit statement of non-consent lifts the burden from them of worrying all the time if they have tended to the device at intimate moments. For a device whose marketing slogan is convenience, the protections proposed in AB 1262 are exactly that, a customer convenience.

However, it remains unclear why the author has elected to limit the bill to voice recognition features on smart speakers, rather than voice recognition features on devices more generally. It is true that the universe of devices containing these features is diverse, and such diversity could raise technical considerations beyond those appropriately considered by the bill in print. Nonetheless, there does not appear to be a qualitative difference between the data collected by voice recognition features on smart speakers compared with the data collected by the same features on, for instance, cellular devices with virtual assistants.

Indeed, a coalition of business advocacy groups in opposition to the bill argue:

> AB 1262 does not provide consistent protections for consumers using voice recognition technologies across all devices. The bill is limited to specific hardware, which conflates hardware (smart speaker devices) with software (voice recognition features). Specifically, the bill seeks to regulate voice recognition features, but fails to regulate it across all devices that provide voice recognition features. This would result in discrimination among business models and technologies and mass confusion for consumers about which voice recognition devices are covered. The bill requires rigid disclosures and mandates that businesses provide service even when consumers decide not to give consent for use of voice recordings, which would also further result in inconsistent consumer experiences and protections in using voice recognition features across various devices.

Accordingly, if the bill passes out of this Committee, as the bill moves through the legislative process, the author may consider how the bill might be expanded to provide for parity for protections related to voice recognition features across devices. Nonetheless, the bill as it is in print appears to provide substantial protections for consumers with respect to any PI collected by the voice recognition features of smart speakers, and would seemingly improve upon the status quo protections generally afforded under the CCPA. Considering the unique sensitivity of voice recording data that could be collected by these devices, either incidentally or intentionally, it is arguably appropriate to provide for such additional protection for PI in this particular case.

8) **Specific language used to define "affirmative written consent" may be overly prescriptive and lead to confusion**: AB 1262 defines "affirmative written consent" to mean that "a manufacturer of a connected television or smart speaker device provided the following disclosure to a user during installation of a device, separate from the device terms

of use, and received authorization from the user pursuant to the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.) and the Uniform Electronic Transactions Act (Title 2.5 (commencing with Section 1633.1) of Part 2 of Division 3 of the Civil Code):

> "*This device may be used to process and retain user recordings and transcriptions of spoken words. Those recordings may be analyzed and shared with third parties by the manufacturer and its employees for the purpose of improving the device. Please indicate whether or not you give your consent for the device to be used in this way. This consent is not required to use basic functions of this device.*
>
> *I authorize [manufacturer name] to share my recordings, and I understand that the recordings may be analyzed and shared with third parties by the manufacturer and its employees.*
>
> *I do not authorize [manufacturer name] to share my recordings and I do not want to have access to the enhanced smart features of this device.*"

Staff recognizes the author's intent to ensure that the request for consent is understandable and contains specified information. However, in its current form, this prescriptive language seems overly rigid, and unlikely to provide the most useful and straightforward prompt to the consumer.

As the opposing coalition points out:

> AB 1262 dictates the exact format and verbiage that businesses must provide to obtain user consent. Depending on the device and how it is used, the required consent mandated in the bill may be both under and over inclusive of meaningfully informing users how the recordings will be used and, in some instances, may require companies to provide incorrect information, thereby misleading consumers. Specifically, the required consent language has a multitude of issues. It implies statutory requirements not found elsewhere in the bill and it requires that business provide users with "the basic functions of the device" even if they do not give consent to the use of their voice recordings. It does not provide a definition of "basic function", and does not recognize that it is not likely to be technologically feasible for smart speaker devices to work without collecting and using the voice recordings. In sum, the consent language does not allow businesses to fairly inform users of what the devices do, how the recordings will be used, and it requires different levels of service that are indecipherable.

Staff further notes that the language for declining consent to share recordings is inextricably linked to declining the enhanced smart features of the device (i.e. "I do not authorize [manufacturer name] to share my recordings *and* I do not want to have access to the enhanced smart features of this device"), depriving a user who does not want their information shared with third parties of the option to continue receiving enhanced smart features of the device, however defined, if the technology allows. For this reason, the author may consider providing specific criteria of clarity and content that the request for consent must meet, without prescribing such inflexible, and potentially misleading, specific language. An amendment to that effect would likely provide further clarity for compliance with the bill, and would strengthen the already extensive consumer protections the bill seeks to provide.

REGISTERED SUPPORT / OPPOSITION:

Support

Common Sense
Oakland Privacy

Opposition

Billion Strong
California Chamber of Commerce
Civil Justice Association of California
Consumer Technology Association
Internet Association
Ruh Global IMPACT
TechNet

Analysis Prepared by: Landon Klein / P. & C.P. / (916) 319-2200