Date of Hearing: April 23, 2019

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 873 (Irwin) – As Amended March 25, 2019

SUBJECT: California Consumer Privacy Act of 2018

SUMMARY: This bill would narrow the definition of personal information (PI) in the California Consumer Privacy Act of 2018 (CCPA) to: (1) exclude information that "is capable of being associated with" a particular consumer; (2) exclude information that could be linked to particular "households"; and, (3) potentially exclude items that are otherwise listed as types of PI even if those items actually identify a particular consumer. This bill would also revise a provision of the CCPA prohibiting the act from being construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered PI. Lastly, this bill would replace the CCPA's current definition of "deidentified." Specifically, **this bill would**:

1) Redefine "deidentified" for purposes of the CCPA to mean information that does not reasonably identify, or link, directly or indirectly, to a particular consumer, provided that the business makes no attempt to reidentify the information, and takes reasonable technical and administrative measures designed to:

   - Ensure that the data is deidentified.

   - Publicly commit to maintain and use the data in a deidentified form.

   - Contractually prohibit recipients of the data from trying to reidentify the data.

2) Redefine "PI" to generally mean information that identifies, relates to, describes, or could reasonably be linked, directly or indirectly, with a particular consumer.

3) Narrow the CCPA definition of PI, further, to state, instead, that PI "may include" (as opposed to "includes"), but is not limited to, certain types of information, as listed under that definition to include, among other things, geolocation information, commercial information, or unique identifiers such as social security numbers, if such information identifies, relates to, describes, or could be reasonably linked, directly or indirectly, with a particular consumer.

4) Revise the provision of the CCPA that exempts businesses from any obligation to reidentify or otherwise link information that is "not maintained in a manner that would be considered PI," to state, instead, that the CCPA shall not be construed to require a business to reidentify or otherwise link information that is "not maintained in personally identified form."

5) Make other technical and non-substantive changes.

EXISTING LAW:

1) Establishes the CCPA and provides various rights to consumers pursuant to the act. Subject to various general exemptions, a consumer has, among other things:

- the right to know what PI a business collects about consumers, as specified, including the categories of third parties with whom the business shares PI, and the specific pieces of information collected about the consumer;

- the right to know what PI a business sells about consumers, as specified, including the categories of PI that the business sold about the consumer and the categories of third parties to whom the PI was sold, by category or categories of PI for each third party to whom the PI was sold;

- the right to access the specific pieces of information a business has collected about the consumer;

- the right to delete information that a business has collected from the consumer;

- the right to opt-out of the sale of the consumer's PI if over 16 years of age, and the right to opt-in, as specified, if the consumer is a minor; and,

- the right to equal service and price, despite exercising any of these rights. (Civ. Code Sec. 1798.100 et seq.)

2) Generally requires under the CCPA that a business subject to the CCPA do all of the following, among other things: comply with the above requirements, provide various notices to those ends, and execute various requests upon receipt of a verifiable consumer request, as specified; and provide certain mechanisms for consumers to make their lawful requests, including a clear and conspicuous link titled "Do Not Sell My Personal Information" on the business's internet homepage to enable consumers, or a person authorized by the consumer, to opt-out of the sale of the consumer's PI. (Civ. Code Sec. 1798.100 et seq.)

3) Provides businesses with various exemptions from their obligations under the CCPA. Of particular relevance to this bill, existing law states that the CCPA shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered PI. (Civ. Code Sec. 1798.145(i).)

4) Provides various definitions under the CCPA. The CCPA, of particular relevance for this bill defines the following terms:

   - "PI," in relevant part, means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. PI includes certain specific types of information, if that information identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household. These include, for example:

     - Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

     - Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

- Geolocation data.

- Inferences drawn from any of the information identified in the definition of PI to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

- "Deidentified" means 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:

  - Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

  - Has implemented business processes that specifically prohibit reidentification of the information.

  - Has implemented business processes to prevent inadvertent release of deidentified information.

  - Makes no attempt to reidentify the information. (Civ. Code Sec. 1798.140.)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of the bill**: This bill seeks to revise or replace various definitions in the CCPA and to otherwise clarify the CCPA provision that narrows the obligation of a business to reidentify or relink information. This bill is sponsored by a coalition of business groups led by the California Chamber of Commerce (CalChamber).

2) **Author's statement**: According to the author:

   This bill addresses critical operational uncertainties in the CCPA, including the range of data subject to its requirements and what steps businesses should take to de-identify data. CCPA requirements are highly operational and the scope of information regulated under the law requires clarification well before the law takes effect on January 1, 2020, as conscientious businesses are already working hard to build compliance programs and implement significant change management, and usually must map data in scope under the law to come into compliance by then. The CCPA is primarily focused on the ability of consumers to assert control over their personal information, and meeting consumer expectations about what the Legislature promised them will be key. By addressing a key practical compliance issue, the Legislature would provide more clarity and efficiency which will ultimately result in a better consumer experience with CCPA. […]

   First, the bill modifies the definition of "personal information" by striking the clause "is capable of beings associated with", striking references to "household", and making the grammatical clarification that the subsequent subsections of categories "may include" as they are dependent upon a conditional clause "if it identifies, relates to, describes…"

Second, the bill restructures the definition of "de-identified" to more closely follow the FTC's 2012 Privacy Framework understanding of "de-identified". The current definition closely but inversely mirrors the current definition of "personal information" which includes the term "capable". The FTC definition focuses on a "reasonably linkable" standard that is qualified by the three elements included in AB 873.

Third, the bill clarifies the CCPA's express directive that it not be interpreted to require a business to re-link data, to apply to "personally identifiable" information rather than "not maintained in a manner that would be considered personal information."

3) **Adding ambiguity in the definition of PI where none currently exists**: Last year, this Legislature enacted the CCPA (AB 375, Chau, Ch. 55, Stats. 2018), which gives consumers certain rights regarding their PI, including: (1) the right to know what PI that is collected and sold about them; (2) the right to request the categories and specific pieces of PI the business collects about them; and (3) the right to opt-out of the sale of their PI, or opt-in in the case of minors under 16 years of age. The final version of the CCPA adopted by the Legislature was the byproduct of compromises made between business interest on the one side, and consumer and privacy interests on the other, to provide a legislative alternative to a ballot initiative on the same subject. Given the abbreviated deadline to formally adopt the CCPA in time for the proponents to remove their proposal from consideration, numerous drafting errors were contained in the legislation as initially adopted. Many of those errors (but not all) were addressed in a preliminary clean-up bill at the end of the 2017-2018 legislative session, in SB 1121 (Dodd, Ch. 735, Stats. 2018). SB 1121 also provided clarification on several items, including on the definition of PI, which is at the center of this bill.

Under the CCPA, all consumer rights and the businesses' corresponding obligations, are dependent upon whether or not certain data constitutes "PI." If it is not "PI," none of the provisions establishing various rights for consumers have any effect in relation to that particular information. Stated another way, a consumer does not have the right to know what information a business collects/sells about them, or to delete or opt-out of the sale of such information in the possession of a business, if the information is not *personal* and identifiable to the consumer.

Generally speaking, the CCPA defines what information is personal is as follows: PI is that information which identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. (*See* Civ. Code Sec. 1798.140(o)(1).) The CCPA definition of PI then proceeds to include a list of items that are deemed "PI," but *only* insofar as those items "identify, relate to, describe, are capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household." Those items include, for example: geolocation information; IP address; unique identifiers such as a social security number, driver's license number, passport number, or email address; and more. Staff notes that when this definition was originally enacted by AB 375, there was no such limiting language around the list. Originally, the limitation was inferred from the general definition. That limitation, however, was expressly clarified in SB 1121, due to industry concerns that an inference was not enough and the itemized types of information would automatically be deemed PI, even if those items did not identify a particular individual.

Now, however, this bill seeks to state that those same items, only *"may"* be considered to constitute PI. In other words, *even* if an item of information identifies an individual, it might not be treated as PI by a business under this bill. Thus, this bill introduces ambiguity into the definition of PI where none currently exists, and in doing so, may very well erode the scope of information that is considered PI and subject to consumer rights. Currently, under the CCPA, as long as that information identifies a person or household, it is definitively PI and the consumer has rights. Now, under this bill, it would only potentially be PI and the consumer may or may not have rights, and the business is left to determine unilaterally whether it will treat that information as PI.

As such, if this Committee were to approve this bill, it should arguably strike the phrase "may include" and reinsert the word "includes" to remove this ambiguity.

Suggested amendment:

On page 6, line 36, strike "may include" and insert "*includes*"

4) **Information that is capable of being associated with a person**: Again, the CCPA generally defines PI as information that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." This bill proposes to eliminate from the definition PI any information that is "capable of being associated with" a particular person or household. (*See* Comment 5 for more on how this bill also seeks to exclude information that identifies particular households from the definition.) In justification of this change, the author writes:

> Most people think of personal information as data that on its own could identify someone, like names or social security numbers. […] The current definition of "personal information," drawn from an obscure record destruction provision added to the California Civil Code in 2000 and used nowhere else in California law, is overbroad and applies CCPA obligations to information that will never in fact be made identifiable, and has no effect on the privacy of consumers. *See* Cal. Civ. Code [Sec.]1798.80. The important distinction between "capable of" and the other terms in the definition -- "identifies" "relates to" "describes" "reasonably be linked" is that there is a strong argument that *all* information is theoretically "capable" of being associated with some other data. Whereas the other terms focus on the current state of the information, the "is capable of" standard is a future consideration that is not even qualified by what is "reasonable". It requires all California businesses to contemplate the ability of the information to associate with a consumer even though it may not currently, a future consideration. The definition of "personal information" without "capable" would still protect the information if those future considerations were born out, and the information did "identify" "relate to" "describe" or "link" to a consumer, but would not encompass information that did not actually pose a privacy risk and "identify" "relate to" "describe" or "link" to a consumer.
>
> […] Putting this into context, if a customer has an online account with a store and exercises their rights under CCPA, that store should be able to provide them with account details or to delete their information. But that's only the beginning of what a business is required to do under this law. Very commonly, a customer also browses sales on a store's website without logging in. If that store keeps IP addresses for web analytics, but it doesn't link that data back with a person - under the CCPA, in response to a consumer

> request, the store could be required to search for every possible IP address they have that could in theory be linked back to a particular consumer. Similarly, if a customer made purchases at the business' brick and mortar store, under the current language of the CCPA, that store could be required to search security camera footage to find where the customer appears on it – and provide it back to the consumer or delete it, depending upon the request – even if the store was never linking that security camera footage back to a consumer. Why? Because the store IS CAPABLE OF ASSOCIATING this data with a particular consumer – and, therefore, arguably must do so under the current construction of the law. This is an unreasonable burden on businesses and unnecessary to advance privacy interests.
>
> […] If businesses face significant operational burden or significant potential liability for honest mistakes missing some data in response to a request, businesses will be incentivized to combine all personal data into data lakes or other centralized repositories in order to be able to comply readily and more reliably with consumer requests. This sort of data combination actually disserves privacy by making information more identifiable and making it easier for businesses to use for additional purposes, instead of leaving it separated and unused for secondary purposes. […].

First, with regard to fears that businesses may face significant potential lability for honest mistakes, Staff notes that, by and large, violations would be subject to actions brought by the Attorney General (AG), who, as a matter of resources, will have to exercise discretion as to the cases warranting action. Thus, the argument that businesses will face significant potential lability is unlikely to come to fruition. Second, the removal of this phrase from the definition of PI arguably erodes the protections of the CCPA. Indeed, Californians for Consumer Privacy opposes the narrowing of the definition of PI, writing that "[t]he definition of personal information is a cornerstone of the CCPA and one of the key provisions that defines the scope of the consumer rights […]" and draws from existing provisions of California law. Similarly, a coalition of consumer and privacy organizations including Common Sense Kids Action (CSKA), Electronic Frontier Foundation (EFF), and the American Civil Liberties Union (ACLU) write in opposition that changes to the definition of PI (as well as deidentified, as discussed further in Comment 6, below) would "undermine necessary privacy protections under the CCPA."

Arguably, a better balancing of the public policy considerations regarding this issue may be reflected by, instead, stating that the information is "*reasonably* capable of being associated with" – similar to how the definition includes information that can be "reasonably linked, directly or indirectly, with" a particular consumer or household. This should, by and large, address the operational concerns raised by the author and proponents. To this end, the Californians for Consumer Privacy writes that it is "open to qualifying the 'capable of being associated with' phrase by including 'reasonably.'"

As such, if this Committee were to approve this bill, it may wish to amend the bill to reinstate the "capable of" phrasing with a "reasonableness" standard as suggested above:

> Suggested amendments:
>
> On page 6, in both lines 33 and 37, after "describes," insert "*is reasonably capable of being associated with,*"

5) **Information that identifies a particular household**: By striking the term "household" from the definition of PI in the CCPA, this bill also seeks to remove protections under the CCPA for any information that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular […] household." The author writes that this change is necessary because "the CCPA's references to households in the definition of personal information presents serious privacy risks. As drafted, one member of a household – whether they are an abusive spouse or a roommate – seems to be able to access all of the specific pieces of information – including credit card info or precise geolocation data – about another member of their household. For example, a household member may request access to specific pieces of information from a grocery store delivery service, thereby exposing another household member's purchase of sensitive items, like a roommate's pregnancy test. Similarly, one user of a household device can request all of the specific pieces of information a company has about that particular household device, which could reveal private things about another user of the device, including for example, a roommate's locations outside a group house. The inclusion of households could also infringe on the choices of others. For example, if one household member makes a request to delete all data associated with a household, another household member would be subsequently unable to access their information." (Emphasis in original.)

   In support, the Nonprofit Alliance writes that it is concerned with elements of the CCPA that may undermine privacy:

   > For example, the law requires disclosure about a consumer to other consumers in that same household. This is not always safe. Someone may have a search history regarding the LGBT community, but perhaps being out is not safe in that household.
   >
   > Further, someone in the household may google information about abortion or birth control services or spousal abuse shelters or support groups—again, that may not be safe information to disclose to others in a household.
   >
   > We appreciate and respect the intent of the CCPA and do not wish to unravel it. Nonprofits are and historically have been good stewards of personal information. Privacy and donor trust with data are priorities to us. It is for this reason we believe the household issue can be fixed[…]."

   That being said, arguably, there are ways to address the concerns raised by the author and proponents that would not require a deletion of "households" from the realm of what might be considered PI under the CCPA. First, a business must receive a verifiable consumer request (VCR) before responding to a request for specific pieces of information. As such a great deal of those issues can potentially be dispensed with depending on the standards set by the AG's regulations as to what constitutes a VCR. Potentially, the AG could require a higher threshold as to what is needed to constitute a VCR in relation to household information.

   Second, if a statutory solution is necessary irrespective of how the AG develops the regulations around VCRs, it is unclear that narrowing the definition of the types of PI that are subject to consumer protections under the CCPA is the most reasonable approach to resolving this issue. Similar to this bill's proposal to remove information that is "capable of being associated with" a particular individual or household from the scope of the CCPA, the removal of "households" from the PI definition would also represent an erosion of the CCPA by narrowing the realm of information subject to CCPA protections. Indeed, to the extent

that there are concerns relating to the vulnerabilities created by requiring businesses to provide consumers access to their specific PI, and PI might be related to other members of a household, AB 25 (Chau) reflects the intent to work with all interested stakeholders to find a solution that would ensure that businesses comply with the obligation to provide specific pieces of information in a privacy protective manner. Both Californians for Consumer Privacy and the coalition including groups such as ACLU, EFF, and CSKA oppose this bill's proposal to remove "households" from the definition of PI.

As such, if this Committee were to approve this bill, it may wish to reinsert the term "households" to avoid the elimination of the CCPA's protections for information that identifies particular households and thereby focus conversations on how to find a privacy protective solution that does not erode the CCPA – a path forward that is offered by AB 25 (Chau).

Suggested amendment:

On page 6, in both lines 35 and 39, after "consumer" insert "*or household*"

6) **Redefining "deidentified"**: This bill seeks to replace the CCPA's definition of "deidentified." Specifically, under the CCPA, "deidentified" means 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 complies with the following safeguards:

- Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
- Has implemented business processes that specifically prohibit reidentification of the information.
- Has implemented business processes to prevent inadvertent release of deidentified information.
- Makes no attempt to reidentify the information.

These safeguards are added to the general definition of "deidentified" (*i.e.*, information that cannot reasonably identify a particular consumer) in recognition of the fact that deidentified information can often be reidentified and that the business must have technical and internal business processes in place to ensure the information remains "deidentified" and prevent the reidentification of that information either internally within the business, or by third parties or service providers with whom the business shares the information.

This bill seeks to now redefine the term to mean information that does not *reasonably identify, or link, directly or indirectly,* to a particular consumer, provided that the business makes no attempt to reidentify the information, and takes reasonable technical and administrative measures designed to:

- Ensure that the data is deidentified.

- Publicly commit to maintain and use the data in a deidentified form.

- Contractually prohibit recipients of the data from trying to reidentify the data.

In many respects, the definition under the CCPA and the definition under this bill align in their mandated safeguards. A coalition of consumer and privacy organizations, including CSKA, EFF, and the ACLU, argue however that this bill eliminates three critical safeguards in the definition of "deidentified" which will "undermine internal processes that protect information against reidentification. The CCPA requires that deidentified information must be accompanied by technical and business safeguards that protect information against reidentification. […] By removing these restrictions, AB 873 puts personal information at risk." CalChamber argues that the amendments to the definition are drawn from the definition of deidentified data from the FTC's 2012 Privacy Report drafted under the Obama Administration, which uses a definition of data that is "reasonably linkable." CalChamber argues that this approach "has been and remains a widely accepted, good practice. It incentivizes sound data-deidentification practices […]."

In terms of the safeguards, the FTC 2012 report states that data is *not* considered "reasonably linkable" to a consumer to the extent that a company (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to reidentify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data. As further described in the report:

> First, the company must take reasonable measures to ensure that the data is de-identified. This means that the company must achieve a reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device. […]
>
> Second, a company must publicly commit to maintain and use the data in a de-identified fashion, and not to attempt to re-identify the data. Thus, if a company does take steps to re-identify such data, its conduct could be actionable under Section 5 of the FTC Act.
>
> Third, if a company makes such de-identified data available to other companies – whether service providers or other third parties – it should contractually prohibit such entities from attempting to re-identify the data. The company that transfers or otherwise makes the data available should exercise reasonable oversight to monitor compliance with these contractual provisions and take appropriate steps to address contractual violations. (FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change* (Mar. 2012) <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> [as of Apr. 17, 2019].)

In an "oppose unless amended" letter, the Californians for Consumer Privacy writes that it does not oppose amending the definition to more closely follow the 2012 FTC definition, as proposed by this bill, but the changes to this definition cannot be taken lightly for several reasons – including because deidentified information is not considered "PI" under the CCPA. To that end, CCP suggests amending AB 873 instead as follows:

> (h) "Deidentified" means information that does not ~~**reasonably**~~ identify ***and is not reasonably linkable,*** ~~**or link**~~ directly or indirectly, to a particular consumer, provided that

the business makes no attempt to reidentify the information, and takes reasonable technical and administrative measures designed to:
(1) Ensure that the data is deidentified.
(2) Publicly commit to maintain and use the data in a deidentified form.
(3) Contractually prohibit recipients of the data from trying to reidentify the data.

As a matter of public policy, this would arguably strike a better balance than the bill, by strengthening the foundational definition of what is considered "deidentified" while following the 2012 FTC order's safeguards more closely:

Suggested amendments:

On page 5 line 19, strike "reasonably" and after "identify" insert "*and is not linkable,*"

On page 5, line 21 strike "or link,"

7) **The term "personally identified form" is unclear, undefined, and potentially undermines the privacy goals of the CCPA**: This bill seeks to provide clarity as to the responsibility of businesses to reidentify certain information. As currently drafted, the CCPA seeks to provide assurance in several provisions that information that is maintained in a deidentified or aggregate form does not have to be relinked to a particular consumer. This arguably encourages privacy protective practices by businesses by incentivizing them to maintain information in formats that cannot reasonably identify an individual – particularly given the extra steps that a business must take for information to qualify as being "deidentified" under the law. (*See* Comment 6, above.) Maintaining information in a non-identifiable form that can still readily be connected to a particular individual, however, is not sufficient under the CCPA – for example, such as when information is maintained in pseudonymized form.

Specifically, to achieve these goals, the CCPA states in the section granting consumers the right to access their PI, the section granting consumers the right to know what PI is collected about them, and the section providing businesses certain exemptions from the CCPA, that a business is not required to "reidentify or otherwise link information that is not maintained in a manner that would be considered [PI]." (In the section granting consumers the right to know, there is a slight variation to this, wherein the provision states the business is not required to "reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered [PI]."

This bill would amend this provision in the section governing businesses' general exemptions to state, instead, that a business is not required to "reidentify or otherwise link information that is not maintained in *personally identified form*." That being said, as echoed in the CCP's "oppose unless amended" letter, the bill, problematically, provides no definition of the term "personally identified form." As a result, it is unclear how that term differentiates from PI, or, inversely, how information that is *not* maintained in "personally identified form" would differ from "deidentified" information or "aggregate consumer information," both of which carry specific meanings under the CCPA. (*See e.g.,* the requirements that must be met for PI to be considered PI, as discussed in Comment 6, above.). In contrast, any information that is not, on its face, identified to a particular individual would presumably not be considered to be in "personally identified form" – even if that information might be sitting in a database,

right next to other information that clearly links it to the particular individual. This would lead to a clear erosion of a consumer's rights under the CCPA.

Staff notes that, to the degree that there is confusion as to what may be considered information that "is not maintained *in a manner that would be considered* PI", the issue could be resolved by simply restating that there is no obligation to reidentify or link information that is "is not maintained *as* PI." Under the CCPA, the definition of PI expressly states that PI is not information that is "deidentified or aggregate consumer information." Staff notes that there is a drafting error in the CCPA, in this regard, but two bills (AB 1355 (Chau) and AB 874 by this same author) seek to correct that error.

In its "oppose unless amended" letter, CCP similarly objects to this change. Whereas the CCPA already "ensures that businesses are not required to take steps to reidentify information, which could be less privacy protective of consumers," CCP argues that "[t]he proposed phrase 'personally identified form' is not defined in the statute and is not appropriate. Given the above proposed changes to 'deidentified' and 'personal information' this change is unwarranted and should be removed."

If this Committee were to approve this bill, it should replace this ambiguous and overly broad phrasing ("not maintained in personally identified form") with "*not maintained as PI*," to better align with the intended operation of this provision in the CCPA.

Suggested amendment:

On page 15, on line 6, strike "in", and on line 8, strike "personally identified form" and insert "*as personal information*"

8) **Other arguments in support**: The sponsor of this bill, CalChamber, writes:

> Personal information is commonly understood to be data that on its own could identify someone, like names or social security numbers. State and federal laws have long reflected this understanding. The CCPA departs from this by defining "personal information" far more broadly, as "information that … identifies, relates to, describes, is capable of being associated with, or could reasonably be linked to … a particular consumer or household." […]
>
> The breadth of the "personal information" definition raised significant operational concerns in the context of the Initiative's focus on selling, but became totally unworkable in the context of the much broader CCPA requirements. In the selling context, businesses presumably combine information that they sell and would know what they are selling. However, this same definition of personal information in the context of access, portability, and deletion rights raises very difficult compliance problems because, in those contexts, businesses do not combine such data and they may be located across the enterprise.
>
> As drafted, this law requires businesses to locate non-identified, consumer data even if those data are not stored together with identified data or not stored in structured format – as long as such data is capable of being associated with a person. This is not just an unreasonable burden on business. The only way for businesses to ensure their compliance with this overly broad provision in the CCPA would be to proactively identify all people

> interacting with their business and to store their information together in one place (making it more vulnerable to hackers). This would be hugely wasteful and harmful to consumer privacy.
>
> We don't believe this was the result intended. The CCPA has an exemption stating that a business is not required to relink data that is "not maintained in a manner that would be considered personal information." But under the current definition of "personal information" essentially all data that is not aggregated is personal information. So this exemption – as currently drafted – does not provide relief, and AB 873 offers amendments to fix it. […] (Footnotes omitted.)

Staff notes that CalChamber's last argument, that the CCPA's definition of PI includes essentially all data that is not aggregated, is not fully accurate. The CCPA's definition of PI excludes both aggregate consumer data, and deidentified data, as well as publicly available information. While there was a drafting error in the CCPA wherein it states "publicly available" information does not include deidentified information or aggregate consumer information, there are no less than two bills this year that would correct that error: AB 1355 (Chau) and AB 874 (Irwin). Thus, a provision in the CCPA stating that a business has no obligation to reidentify or link information that is not maintained as PI, would necessarily exempt a business from any obligation to reidentify or link deidentified or aggregate consumer information.

9) **Other arguments in opposition**: In addition to its stated concerns with the changes to the "deidentified" definition above, the coalition of consumer and privacy groups including ACLU, EFF, CSKA, Consumer Federation, Privacy Rights Clearinghouse, among others, writes in opposition that the removal of the term "household" from the definition of PI "threaten[s] to undermine protections for information associated with a household (e.g., by an Internet Service Provider or a connected device)." These groups also argue that the bill "removes critical language that ensures that privacy protections for personal information take into account the modern realities of how personal information is stored and used." They write that voters overwhelmingly state that it is important to control information related to or collected by a household – such as where an individual lives, who they live with, or from a device in their home (*e.g.* personal assistant smart devices like Alexa, baby monitors, and "smart" TVs or refrigerators). Ultimately, they argue that "[t]he CCPA's definition of personal information should be maintained." As stated in their letter:

> Privacy laws must take into account the modern reality that anonymization techniques do not adequately protect information. For example, "anonymized" search queries released by AOL were nonetheless associated with particular individuals. And Twitter users were unmasked by leveraging the structure of social relationships. Machine learning techniques can significantly reduce the difficulty of re-identifying personal information over time. Signaling the maturity of these re-identification techniques, data brokers are even offering what is effectively re-identification as a service, promising the ability to "reach customers, not cookies". As written, AB 873 threatens to eliminate protections for information that has immense potential to violate people's privacy.

10) **Related legislation**: AB 25 (Chau) seeks to clarify the CCPA's definition of consumer and how businesses may comply with a consumer's request for specific pieces of information in a privacy protective manner under the CCPA. This bill is pending hearing in this Committee.

AB 288 (Cunningham) seeks to establish laws governing "social media privacy" separate and apart from the CCPA's existing requirements for such companies that meet the "business" definition thresholds identified in the CCPA. Specifically, the bill would require a social networking service, as defined, to provide users that close their accounts the option to have the user's "personally identifiable information" permanently removed from the company's database and records and to prohibit the service from selling that information to, or exchanging that information with, a third party in the future, subject to specified exceptions. The bill would require a social networking service to honor such a request within a commercially reasonable time. The bill would authorize consumers to bring private right of action for a violation of these provisions, as specified. This bill has been referred to this Committee.

AB 523 (Irwin) seeks to address the sale of geolocation information by certain businesses, separate and apart from the CCPA's existing requirements and restrictions governing companies that meet the "business" definition thresholds identified in the CCPA and seek to sell their consumers' PI (which the CCPA defines to include geolocation information). This bill is pending hearing in the Assembly Communications and Conveyance Committee.

AB 846 (Burke) seeks to replace "financial incentive programs" provisions in the non-discrimination statute of the CCPA with an authorization for offerings that include, among other things, gift cards or certificates, discounts, payments to consumers, or other benefits associated with a loyalty or rewards program, as specified. This bill is pending hearing in this Committee.

AB 874 (Irwin) seeks to broaden the definition of "publicly available" for purposes of the PI definition, which excludes "publicly available" information. The bill would also correct a drafting error in the definition of "PI" to clarify that PI does not include deidentified or aggregate consumer information. This bill is pending hearing in this Committee.

AB 981 (Daly) would add numerous privacy protections to the Insurance Information and Privacy Protection Act (IIPPA), to reflect the CCPA. The bill would exempt entities subject to the IIPPA, as specified, from the CCPA, with the exception of the CCPA's data breach section. This bill is pending hearing in this Committee.

AB 1035 (Mayes) seeks to require, under the Data Breach Notification Law, a person or business, as defined, that owns or licenses computerized data that includes PI to disclose any breach of the security of the system within 72 hours following discovery or notification of the breach, subject to the legitimate needs of law enforcement, as provided. This bill is pending hearing in this Committee.

AB 1138 (Gallagher) seeks to prohibit a person or business that conducts business in California, and that operates a social media website or application, from allowing a person under 16 years of age to create an account with the website or application unless the website or application obtains the consent of the person's parent or guardian before creating the account. This bill is pending hearing in this Committee.

AB 1146 (Berman) seeks to expand the CCPA exemptions to expressly exclude from the CCPA vehicle information shared between a new motor vehicle dealer and the vehicle's manufacturer, if the information is shared pursuant to, or in anticipation of, a vehicle repair

relating to warranty work or a recall, as specified. This bill is pending hearing in this Committee.

AB 1355 (Chau) seeks to address a drafting error in the definition of PI to clarify that it does not include deidentified or aggregate consumer information. This bill is pending hearing in this Committee.

AB 1395 (Cunningham) seeks to prohibit a smart speaker device, as defined, or a specified manufacturer of that device, from saving or storing recordings of verbal commands or requests given to the device, or verbal conversations heard by the device, regardless of whether the device was triggered using a key term or phrase. This bill is pending hearing in this Committee.

AB 1416 (Cooley) seeks to expand the CCPA exemptions to specify that the act does not restrict a business's ability comply with any rules or regulations. The bill would also expand the CCPA existing exemptions, which already include that the act does not restrict a business's ability to exercise or defend legal claims, to instead specify that the act does not restrict a business's ability to collect, use, retain, sell, authenticate, or disclose PI: (1) in order to exercise, defend, or protect against legal claims; (2) in order to protect against or prevent fraud or unauthorized transactions; (3) in order to protect against or prevent security incidents or other malicious, deceptive, or illegal activity; (4) in order to investigate, report, or prosecute those responsible for protecting against fraud, unauthorized transactions, and preventing security incidents or other specified activities; or, (5) for the purpose of assisting another person or government agency to conduct the aforementioned activities. This bill is pending hearing in this Committee.

AB 1564 (Berman) would revise a requirement in the CCPA for businesses to make available to consumers "two or more designated methods" for submitting requests for information to be disclosed pursuant to specified provisions of the CCPA, including, at a minimum, a toll free telephone number and, if the business maintains an internet website, a website address. This bill is pending hearing in this Committee.

AB 1760 (Wicks) would restate the CCPA rights using similar terminology, expand those existing CCPA rights to include new rights, and replace the "opt-out" rights of consumers 16 years and older with an "opt-in" right, among other things. This bill is pending hearing in this Committee.

11) **Prior legislation**: AB 375 (Chau, Ch. 55, Stats. 2018) *See* Comment 3.

SB 1121 (Dodd, Ch. 735, Stats. 2018) ensured that a private right of action under the CCPA applies only to the CCPA's data breach section on and not to any other section of the CCPA, as specified, corrected numerous drafting errors, made non-controversial clarifying amendments, and addressed several policy suggestions made by the AG in a preliminary clean-up bill to AB 375.

REGISTERED SUPPORT / OPPOSITION:

Support

California Chamber of Commerce (sponsor)

Advanced Medical Technology Association (Advamed)
Association of National Advertisers
California Asian Pacific Chamber of Commerce
California Bankers Association
California Cable & Telecommunications Association
California Fuels and Convenience Alliance
California Hispanic Chambers of Commerce
California Hospital Association
California Land Title Association
California Life Sciences Association
California Mortgage Bankers Association
California News Publishers Association
California Restaurant Association
California Retailers Association
Card Coalition
Computing Technology Industry Association
Consumer Data Industry Association
Consumer Technology Association
CTIA-The Wireless Association
Email Sender and Provider Coalition
Entertainment Software Association
Insights Association
Internet Association
Investment Company Institute
National Federation of Independent Business
Network Advertising Initiative
Securities Industry and Financial Markets Association
Technet
The Nonprofit Alliance

Opposition

Access Humboldt
Californians for Consumer Privacy (unless amended)
Center for Digital Democracy
Common Sense Kids Action
Consumer Federation Of California
Consumer Reports
Digital Privacy Alliance
Electronic Frontier Foundation
Media Alliance
Oakland Privacy
Privacy Rights Clearinghouse

Analysis Prepared by: Ronak Daylami / P. & C.P. / (916) 319-2200