

Date of Hearing: April 30, 2019

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION

Ed Chau, Chair

AB 1416 (Cooley) – As Introduced February 22, 2019

**SUBJECT:** Business: collection and disclosures of Consumer personal information

**SUMMARY:** This bill would expand the exemptions to the California Consumer Privacy Act of 2018 (CCPA), as specified. Specifically, **this bill would:**

- 1) Specify that the obligations imposed on businesses by the CCPA shall not restrict a business's ability to comply with any rules or regulations.
- 2) Expand the current exemption for exercising or defending legal claims to instead allow businesses to collect, use, retain, sell, authenticate, or disclose personal information (PI) in order to do any of the following:
  - Exercise, defend, or protect against legal claims.
  - Protect against or prevent fraud or unauthorized transactions.
  - Protect against or prevent security incidents or other malicious, deceptive, or illegal activity.
  - Investigate, report, or prosecute those responsible for any activity set forth in the preceding two paragraphs.
- 3) Add a new exemption specifying that the obligations imposed on businesses by the CCPA shall not restrict a business's ability to collect, use, retain, sell, authenticate, or disclose a consumer's PI for the purpose of assisting another person or government agency to conduct any of the activities specified directly above.

**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 VCR, 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 that a consumer has the right to request that a business delete any PI about the consumer which the business has collected from the consumer, subject to specified exceptions. Specifically, a business or a service provider are not required to comply with a consumer's request to delete the consumer's PI if it is necessary for the business or service provider to maintain the consumer's PI in order to, among other things:
- 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 otherwise perform a contract between the business and the consumer.
  - Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
  - Debug to identify and repair errors that impair existing intended functionality.
  - Comply with the California Electronic Communications Privacy Act, as specified.
  - Comply with a legal obligation. (Civ. Code Sec. 1798.105, "the right to delete.")
- 4) Grants all consumers over the age of 16 the right, at any time, to direct a business that sells PI about the consumer to third parties not to sell the consumer's PI (the right to "opt-out"). For all consumers less than 16 years of age, prohibits businesses from selling PI unless the consumer (or in the case of consumers under 13 years of age, the consumer's parent or guardian) has affirmatively authorized the sale of the consumer's PI (the right to "opt-in"). (Civ. Code Sec. 1798.120.)
- 5) Provides various exemptions under the CCPA. Specifically:
- Provides that the obligations imposed on businesses by the CCPA shall not restrict a business's ability to do the following, among other things:
    - Comply with federal, state, or local laws.

- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.
  - Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.
  - Exercise or defend legal claims. (Civ. Code Sec. 1798.145.)
  - Provides that the CCPA shall not apply to, among other things:
    - The sale of PI to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report as defined under specified federal regulations, and use of that information is limited by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).
    - PI collected, processed, sold or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), or the California Financial Information Privacy Act (Fin. Code Sec. 4050 et seq.) (Civ. Code Sec. 1798.145.)
- 6) Provides various definitions under the CCPA. The CCPA, of particular relevance for this bill, defines the following terms:
- “Business” means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers’ PI, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ PI, that does business in California, and that satisfies one or more of specified thresholds,
  - “Third party” means a person who is not any one of the following:
    - The business that collects the PI.
    - A person to whom the business discloses a consumer’s PI for a business purpose, pursuant to a written contract that prohibits, among other things, the recipient from selling the PI, or retaining, using, or disclosing the PI outside the direct business relationship between the person and the business.
  - “PI” 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.

- Characteristics of protected classifications under California or federal law.
- Commercial information, as specified.

PI does not include publicly available information, as specified. Among other things specifies that for these purposes, “publicly available” means information that is lawfully made available from federal, state, or local government records, as specified. Information is not “publicly available” if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained.

- “Sell,” “selling,” “sale,” or “sold,” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s PI by the business to another business or a third party for monetary or other valuable consideration. For purposes of the CCPA, a business does not “sell” PI when, among other things:
  - A consumer uses or directs the business to intentionally disclose, as specified, PI or uses the business to intentionally interact with a third party, provided the third party does not also sell the PI, unless that disclosure would be consistent with this bill.
  - The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer’s PI for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer’s PI.
  - The business uses or shares with a service provider PI of a consumer that is necessary to perform a business purpose if both of the following conditions are met: (i) the business has provided notice that information being used or shared in its terms and conditions, as otherwise specified under the bill; and (ii) the service provider does not further collect, sell, or use the PI of the consumer except as necessary to perform the business purpose. (Civ. Code Sec. 1798.140.)

**FISCAL EFFECT:** None. This bill has been keyed nonfiscal by the Legislative Counsel.

**COMMENTS:**

- 1) **Purpose of this bill:** This bill seeks to ensure that public entities can receive data necessary for various programs, services, or purposes after the CCPA takes effect. This is sponsored by the California State Association of Counties.
- 2) **Author’s statement:** According to the author, “AB 1416 will further long-established public policy objectives in that it allows California to continue to operate as expected, providing critical programs and social services when such essential services rely on the use of data from private firms. California’s duty to its people includes assisting state and local law enforcement efforts and fraud prevention, administration of debt recovery, and prioritizing the placement of foster youth with blood-related family. Without this bill, California’s efforts will be undermined and unable to fulfil their intended purpose.”
- 3) **Impact of CCPA on government entities at debate in this bill:** Last year, the Legislature enacted the CCPA (AB 375, Chau, Ch. 55, Stats. 2018), which gives consumers certain rights

regarding their PI, such as: (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; (3) the right to delete PI collected from them; and, (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.

The author argues that, “[a]s a consequence of the CCPA, California’s government agencies fall under the same restrictions as non-government agencies, and businesses will be prevented from sharing collected personal information with a legitimate government program if a consumer opts-out of their data sharing. AB 1416 remedies the CCPA by removing restrictions preventing businesses from sharing personal information of opted-out consumers with government agencies, and removes restrictions preventing the business from doing so in order to comply with state, federal, or local laws and regulations. Additionally, permitting government agencies to access personal data will allow the government to continue operating mandated programs, such as combating identity theft, assisting law enforcement apprehend criminals, and prioritizing the placement of foster youth with blood relatives.”

Under the CCPA, a business is a “sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers’ PI, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ PI, that does business in California, and that satisfies one or more” of three possible thresholds relating to: (1) the business’s gross revenue; (2) the number of consumers, households, or devices, alone or in combination, from which the business, alone or in combination, annually buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes, PI; or, (3) the percentage of their annual revenues that they derive from the sale of consumers’ PI.

A third party is a “person” who is not: (1) the business that collects the PI; or, (2) a person to whom the business discloses a consumer’s PI for a business purpose, pursuant to a written contract that prohibits, among other things, the recipient from selling the PI, or retaining, using, or disclosing the PI outside the direct business relationship between the person and the business. “Person” in turn, means an individual, proprietorship, firm, partnership, [...] and any other organization or group of persons acting in concert.

Government entities are clearly not “businesses.” The question then becomes if they can be a “person” who can then be considered a “third party” for purposes of the CCPA. Arguably, to the extent a state agency, department, or office could be considered “any other organization or group of persons acting in concert,” a government entity could be considered a “person” for purposes of the CCPA’s “third person” definition. In support, the California Alliance of Caregivers also writes that without this bill, “services related to child welfare would be negatively impacted.” Specifically:

In order to achieve the goals of CCR [Continuum of Care Reform], it is imperative that agencies are able to locate family or extended family members who are able and willing to care for their relatives/friends suffering from abuse and neglect. Child Welfare agencies needs to locate potential caregivers quickly so that children do not suffer the additional trauma of moving from one temporary placement to another as the agency struggles to find able and willing family or friends of the child.

For thousands of children awaiting permanency in California, timely access to information could be life changing. If this fix is not made to personal data collection and privacy, the gains that the child welfare system has made to provide the best placements for children entering the child welfare system will be impeded. The definitions provided for in AB 375 do not accurately reflect the relationship between a government entity and the businesses that retain and disseminate critical data. Although government entities are not considered “businesses” under AB 375, they are still third parties with whom businesses can be blocked from sharing information pursuant to a consumer opt-out. The consumer opt-out could mean dropping out of records needed for family finding in Child Welfare agencies.

While locating family and non-related extended family members is indeed critical to the child welfare system, staff notes that the CCPA does not limit information available by way of the California Public Records Act, which is a resource available to all persons, public and private, to obtain government records. Additionally, companies in the business of aggregating information in the provision of government services would be able to share that information with government entities.

That being said, if the concern is to ensure that government programs are not unduly compromised by stifling the flow of information from businesses and data aggregators to government entities, a question is raised as to why the bill does not simply reflect a narrow exemption for governmental entities to obtain information for purposes of governmental programs. Indeed, this bill, instead, seeks to add new exemptions to the CCPA that apply not only to businesses that interact with government entities to provide them with vital data for purposes of government programs, but also to businesses that have no interaction whatsoever with government entities.

- 4) **Exemptions offered by this bill apply much more expansively than necessary to address the author’s intent:** As noted above, this bill is largely premised on concerns about the unintended consequences that the CCPA may have on government agencies carrying forth their government programs, but the solution is not tailored as such. In addition to expanding the CCPA exemptions to specify that the act does not restrict a business’s ability comply with “any rules or regulations” (*see* Comment 6 for more), this bill would expand the CCPA’s existing exemptions to specify that the act does not restrict a business’s ability to collect, use, retain, sell, authenticate, or disclose PI for any of the following:
- in order to exercise, defend, or protect against legal claims (the CCPA already has an exemption for exercising or defending legal claims);
  - in order to protect against or prevent fraud or unauthorized transactions;
  - in order to protect against or prevent security incidents or other malicious, deceptive, or illegal activity;
  - in order to investigate, report, or prosecute those responsible for protecting against fraud, unauthorized transactions, and preventing security incidents or other specified activities;
- or,

- for the purpose of assisting another person or government agency to conduct the aforementioned activities.

Again, nothing within the express language of the above exemptions is limited to facilitating necessary data exchanges between businesses and government entities in furtherance of the latter's legitimate governmental programs or services. Rather, the provisions also apply to businesses who have no interaction with government entities to provide businesses exemptions both within the context of their own internal non-governmental activities, as well when assisting another person to conduct such non-governmental activities. Compare this to another bill this Committee considered very recently, AB 1564 (Berman), which included a limited exemption from the CCPA to enable vehicle manufacturers and car dealers to be able to retain and share data between them, and only them, if that data is necessary for warranty or recall purposes pursuant to federal law.

Here, a business having no interaction with a government agency, could now claim under the proposed changes to this exemptions section, that they need to retain a consumer's PI or share it with other companies in order to "protect against" legal claims or investigate malicious activity, and so forth. (*See* Proposed Section 1798.145(a)(4) and (7).) Such general exemptions to the CCPA are arguably unnecessary and overly broad. For example, *protecting* against legal claims is a much different standard that *exercising* or *defending* legal claims – both of which are appropriately included in the existing CCPA exemptions. (Civ. Code Sec. 1798.140(a)(4).) Put another way, any action that a business takes as a reasonable actor, could be couched as avoiding or "protecting against" legal claims. In opposition, the Californians for Consumer Privacy (CCP) writes:

The expansion of Civil Code Section 1798.145 (a)(4) will authorize a business to take away nearly every consumer right established under the CCPA. The inclusion of the following language would introduce new and broad vagueness within the CCPA, allowing a business to collect, use, retain, sell or disclose a consumer's data for **virtually any purpose**[...].

The inclusion of terms such as "protect against" and "investigate" provide ultimate discretion for a business not to comply with the provisions of the CCPA. As written, this language represents a significant erosion of brand-new consumer rights. In addition, many of the situations raised in AB 1416's new language are already addressed elsewhere in the law. For example, the CCPA already provides exceptions to the title where there could reasonably be a concern regarding legal claims, fraud, security incidents, etc.

Subdivisions (1) through (3) [of the existing CCPA exemptions] provide all the required authority necessary for a business to provide data to law enforcement with respect to potential violations of the law. Subdivision (4) provides all the authority necessary to defend against legal claims. AB 1416's proposed allowance of the collection and sale of personal information simply to, for example, 'protect against...legal claims' or to 'investigate...malicious activity' could theoretically allow the almost unlimited collection and sale of personal information, on the grounds that a business was taking preemptive steps to prepare for a bad outcome.

Additionally, as alluded to in Comment 3, above, even if the bill were to be limited to the context of information sharing between businesses and government agencies, the CCPA

allows for government agencies to obtain a wealth of information from businesses that may be instrumental to their governmental activities – for example, information aggregated from federal, state, or local public records, particularly as proposed to be amended by AB 874 (Irwin), would not constitute PI and would not be subject to sharing restrictions under the CCPA.

Accordingly, if this Committee were to approve this bill, it may wish to strike the new exemptions specified above (under proposed paragraphs (a)(4) and (7)) to, instead, create a narrow exemption that would allow a business to provide a consumer's PI to a public entity for purposes of government programs, consistent with the author's intent. To this end, the following amendments would enable a business to share data in its possession with government entities for purposes of their government programs, even if a consumer opts-out or requests to have their PI deleted by that business, but not for any other purpose. They also ensure that the government agency does not further share or retain the PI for non-programmatic related purposes. Lastly, these amendments would also reinstate the CCPA's existing exemption for a business to "exercise or defend legal claims."

Suggested amendment:

On page 2, strike lines 15-23 and insert: "(4) *Exercise or defend legal claims.*

*(5) Provide a consumer's personal information to a government agency solely for the purposes of carrying out a government program, including providing government services in furtherance of a government program, provided that all of the following requirements are met:*

*(A) the business does not sell the personal information of a consumer who has opted out of the sale of the consumer's personal information for any purpose other than providing it to a government agency for purposes of, and in furtherance of, a government program;*

*(B) the business does not retain the personal information of a consumer who has requested deletion of the consumer's personal information for any purpose other than providing it to a government agency for purposes of, and in furtherance of, a government program; and*

*(C) the government agency shall not further share or retain the information except for purposes of carrying out a government program."*

On page 3, strike lines 6-10, inclusive.

That being said, there remains a fundamental policy question as to whether, and when, government access interests outweigh the consumer's privacy interests. Relatedly, there also remains a public policy question as to whether there should be a limit to how many years the information may be retained for these purposes, once the consumer has opted-out or sought to delete the information. Arguably, the information loses a great deal of utility after a number of years, and a person's privacy interests should outweigh the interest in maintaining that information in the event that it might be useful five, 10, or even 20 years down the line.

- 5) **Exemption for businesses to share information with other businesses to prevent fraud or security incidents:** As noted above, as introduced, this bill not only seeks to allow for



businesses to share PI with government agencies to protect against or prevent fraud or security incidents and other malicious, deceptive, or illegal activities (or investigate such activities), but also to share a consumer's PI with other non-governmental persons for those same purposes. Staff notes that the primary concern stated by the author relates only to government agencies. The amendment in Comment 3, above, achieves those purposes.

That said, many proponents have indicated that security and fraud exemptions are necessary, lest the CCPA allow fraudsters, hackers and other criminals to use the CCPA to opt-out of inclusion of their PI in products offered by fraud and cybersecurity companies. These proponents also argue that fraud prevention is specifically mentioned under the General Data Protection Regulation of the European Union (the EU equivalent to the CCPA). Staff notes that the CCPA already includes provisions specific to fraud and security concerns. Indeed, as noted by the CCP's opposition in Comment 3, under the existing CCPA, non-public entities and persons have the ability to retain information pursuant to an express exemption in the right of deletion. Specifically, the right of deletion specifies that a business or a service provider shall not be required to comply with a consumer's request to delete the consumer's PI if it is necessary for the business or service provider to maintain the consumer's PI in order to "detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity." Further, under the CCPA, businesses have the right to use PI for business purposes that expressly include, again, "detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity." As further noted by CCP in opposition to the bill:

[...] the CCPA contemplated situations where information would need to be shared by a business, even if a consumer elected to exercise their right to opt-out. Under Civil Code Section 1798.140 (d), law defines a "business purpose" which defines situations in which a business may need to share information for an operational purpose. Specifically, that provision reads as follows [in relevant part]:

*Civil Code Section 1798.140 (d) "Business purpose" means the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are:*

*(1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.*

*(2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.*

Thus, we see that as with deletion, Civil Code Section 1798.140 (d) *already* provides solutions to the problems that AB 1416 proposes to 'fix,' especially in subsection (2) above. The CCPA was constructed in a way to provide consumers the right to have

control of their data in a world where data increasingly proliferates through the economy without consumers' consent or control. The law already has important safeguards to prevent fraudulent activity and defend against legal claims. [Emphases in original.]

As such, it is unclear as to why any further exemption is needed here when the CCPA already addresses fraud prevention and security. In fact, expanding the CCPA exemptions in the manner proposed by this bill could very well present a potential loophole in the law, however unintentional. That being said, in support of this bill, a coalition of business groups led by the California Chamber of Commerce (CalChamber) insist that:

The CCPA's opt-out provision also undermines legal compliance activities and efforts by businesses to protect consumers from identity theft and to prevent other crimes, like money laundering and human trafficking, because it contains no exception for the prevention or investigation of fraud or other illegal activities. If not fixed, this would allow bad actors to opt out of services designed to prevent or investigate fraudulent or illegal behavior. [...]

The CCPA already recognizes part of this problem in the deletion section of the law, which has an exemption stating that businesses need not delete data that is necessary to detect security incidents or to protect against malicious, deceptive, fraudulent, or illegal activity. AB 1416 ensures that this same type of exemption can be applied to the right to opt out of the sale of data for these limited purposes.

This fix is necessary because other provisions of the CCPA do not address this concern. Although the definition of business purpose in the CCPA contains an exemption for "detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity," there is no provision stating that by having a statutorily defined "business purpose" a business may refuse to honor an opt-out request.

Further, as discussed in the example above, provisions that exempt some data exchanges between a "Business" and a "Service Provider" from the definition of "sale" do not address the problem either. Companies providing fraud or crime prevention/investigation data services to businesses and governments are not "Service Providers" to those customers under the CCPA. A "Service Provider" is an entity that receives data from a Business and processes it solely for the Business. Instead, companies providing fraud or crime prevention/investigation services are selling data they control to another business or government agency; they are not only processing the data of the business or government agency.

If the Committee and author desire to eliminate remaining confusion on this matter, then the exemption should be limited to mirror the same language provided in the "right of deletion" and the "business purposes" definition, given the concerns that the bill's proposed exemptions are unnecessarily broad and could create loopholes where none exist in the CCPA currently. Any amendment should be narrowly drawn to authorize a business to share with a person the PI of a consumer who has opted-out of the sale of the consumer's PI for the sole purpose of (mirroring those provisions) "detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity," provided that the business and the person shall not further sell that information for

any other purpose. Such a narrow exemption would be tailored to the actual complaint of the CalChamber coalition: that the existing provisions in the right of deletion and business purposes definition for detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity do not apply to situations where the consumer has opted-out of the sale of their PI. Otherwise, this Committee should, as suggested in Comment 4, above, repeal these provisions in their entirety and focus on the author's concern regarding governmental entities and recognition for "rules and regulations," as discussed in Comment 6, below.

- 6) **Exemption for necessary compliance with federal, state, or local laws:** As noted above, among the various exemptions sought by this bill is the addition of an exemption which provides that the obligations of the CCPA shall not restrict a business's ability to comply with any rules or regulations. Currently the CCPA simply states it does not restrict a business's ability to comply with federal, state, or local laws.

In support, Tesla writes "[c]urrently, while the CCPA provides that the Act shall not restrict a business's ability to comply with federal, state, or local laws, it is silent with respect rules or regulations. [...] For example, the California Air Resources Board (CARB) adopted regulations that will authorize electric vehicle (EV) manufacturers, EV charging equipment developers, and load serving entities (electric utilities and Community Choice Aggregators) to earn credits via the Low Carbon Fuel Standard (LCFS) when customers charge their EVs. However, CARB's regulations will require these parties to obtain and report VIN-level data from EV owners for verification purposes, potentially triggering CCPA's requirements to disclose this information as a "sale" of a customer's personal information. This will unfortunately create an onerous and unintended compliance obligation that may frustrate the intent of the LCFS and limit the amount of data available to CARB to audit compliance with the regulation."

CCP argues in opposition that, "it is unclear why the current language in Civil Code Section 1798.145 (a)(1) does not provide sufficient clarity to businesses to ensure that the CCPA will not restrict a business's ability to comply with current law. We have great concerns that the blanket inclusion of rules and regulations, as proposed in AB 1416, will be a vector for nefarious actors to avoid some of CCPA's key consumer protections. We believe this inclusion is expansive and ambiguous, will create confusion and will provide a significant loophole."

Staff notes that adding "any rules or regulations" could undermine the CCPA if, for example, a federal agency or commission were to adopt rules or regulations with the specific intent to undermine the CCPA. While Congress, too, could seek to enact legislation that would preempt the CCPA, passing federal legislation arguably entails greater checks and balances than a commission quietly passing regulations. Furthermore, there is a question as to whether local rules or regulations should ever effectively preempt state law. That being said, the bill actually goes even further than allowing for an exemption for federal, state, or local rules or regulations. It creates an exemption for *any* rules or regulations. In other words, if a company adopted rules or regulations, they could exempt themselves from the CCPA. Such an outcome is untenable.

If this Committee were to approve this bill, the author should continue to work with stakeholders and Committee to ensure that this provision can be narrowed in a manner that

can achieve the stated goal of proponents, without undermining the CCPA. At the very least, the bill should arguably be narrowed to state that the obligations of the CCPA shall not restrict a business's ability to retain or share information as necessary to comply with requirements of federal or state rules or regulations adopted in furtherance of federal or state laws, as follows:

Suggested amendment:

On page 2, lines 5-6, after "or any rules or regulations" insert "*adopted pursuant to and in furtherance of state or federal laws.*"

- 7) **Other arguments in support:** The California Association of County Treasurers and Tax Collectors writes in support that "[t]ax collectors contract with some private entities to research delinquent or defaulted taxpayers, or to conduct other critical work in furtherance of their operations. These contracts produce data needed to successfully implement valuable debt offset and recovery programs in partnership with the California Franchise Tax Board. Private data helps ensure that local agencies are not only notifying the correct resident when multiple residents have the same name, but also ensures that the correct resident has his or her payment accounted for. Absent the passage of AB 1416, collection efforts would be harmed."

The Alliance for Children's Rights supports AB 1416, "to ensure access to information databases by county child welfare workers when seeking emergency placements with relatives to support children removed from their homes as a result of allegations of abuse or neglect. County child welfare workers also utilize such data when undertaking family finding and engagement activities in their diligent efforts to identify, locate and engage appropriate relatives to support children in foster care." Specifically, the Alliance writes, "[f]amily finding and engagement may be compromised as a result of an unintended consequence of the "consumer opt-out" provision enacted in the Consumer Privacy Act of 2018 (Civil Code 1798.105.(a) by interfering with continued appropriate use of complete information databases by child welfare workers when undertaking required efforts to find and engage family members to support children in foster care."

Staff notes that, arguably, the alternative solution offered in Comment 3, above, would address the proponents concerns of the impact the CCPA will have on their programs.

- 8) **Other arguments in opposition:** In opposition, the CCP fundamentally disagrees with the proponents of this legislation over the question of whether government data access should supersede consumer privacy rights.

We recognize that governments have come to rely on the data industry to enhance the administration of various programs. While there may be some areas where data use by government is warranted, authorizing the continued and unfettered operation of the data surveillance economy, even when a consumer has exercised their right to opt-out of the sale of their information, threatens the very essence of right to privacy guaranteed by the California Constitution, and enhanced by the CCPA.

We are greatly concerned that AB 1416 would provide the right for data brokers and other businesses to continue the unchecked collection of consumer data if they are willing

to provide it to a government agency. Unfortunately, we believe this type of allowance would greatly undermine the right for a consumer to opt-out of the sale of their data.

- 9) **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 the Assembly Appropriations Committee.

AB 288 (Cunningham) seeks to establish laws governing “social media privacy” separately 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 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 protect Californians’ privacy with respect to the sale of their geolocation information by telephone corporations. This bill is pending hearing in this 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 the Assembly Appropriations Committee.

AB 873 (Irwin) seeks to revise the CCPA’s definitions of “PI” and “deidentified” and to revise the CCPA’s existing provision that prohibits 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. This bill is pending hearing in the Assembly Appropriations Committee.

AB 874 (Irwin) seeks to revise the definition of “publicly available” for purposes of the PI definition, which excludes such 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 the Assembly Appropriations 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 the Assembly Appropriations 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 13 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 the Assembly Appropriations 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 the Assembly Appropriations 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 the Assembly Appropriations 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, as specified. This bill is pending hearing in this Committee.

AB 1564 (Berman) would revise a CCPA requirement that businesses 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 a toll-free telephone number. This bill is pending hearing in the Assembly Appropriations 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 has been referred to this Committee.

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

## **REGISTERED SUPPORT / OPPOSITION:**

### **Support**

California State Association of Counties (sponsor)  
Alliance for Children's Rights  
California Alliance of Caregivers  
California Association of County Treasurers & Tax Collectors  
California Attractions and Parks Association  
California Bankers Association  
California Chamber of Commerce  
California Credit Union League  
California Land Title Association  
Child Support Directors Association of California  
Civil Justice Association of California  
Computing Technology Industry Association  
Consumer Data Industry Association

CTIA-The Wireless Association  
Electronic Transactions Association  
Entertainment Software Association  
Internet Association  
League of California Cities  
Securities Industry and Financial Markets Association  
Symantec  
Technet  
Tesla  
Thomson Reuters (Markets) LLC, D/B/A Refinitiv

**Opposition**

Californians for Consumer Privacy

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