

Date of Hearing: April 23, 2019

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION

Ed Chau, Chair

AB 1760 (Wicks) – As Amended April 12, 2019

SUBJECT: California Consumer Privacy Act of 2018

SUMMARY: This bill seeks to re-establish the consumer rights and business obligations of the California Consumer Privacy Act of 2018 (CCPA) to be based on the “sharing” of a consumer’s personal information (PI) by a business, instead of the “sale” of a consumer’s PI (which includes sharing if for valuable consideration). This bill would generally modify the rights and obligations of the CCPA to: (1) change the law from an “opt-out” and “opt-in” hybrid dependent on the age of the consumer, to, instead, provide a right for consumers of any age to “opt-in” before a business may share their PI; (2) remove any ability for businesses to provide certain financial incentives that are nondiscriminatory, as specified under the CCPA; (3) limit the use and retention of PI by a business to what is reasonably necessary to provide a service or conduct an activity, as specified, subject to certain exceptions; (4) broaden the duties of businesses in connection with CCPA sections governing the disclosure, access, and deletion of consumer information, while also narrowing certain CCPA exemptions (including exemptions specific to the right of deletion); (5) repeal any right to cure for businesses; (6) repeal the authorization for businesses to seek guidance related to compliance from the Attorney General’s (AG) office; and (7) redefine various terms. This bill would also revise the CCPA’s public enforcement provision to additionally authorize a county district attorney, a city attorney, or a county counsel to bring a civil action, in the name of the of the people of the State of California, against any business, service provider, or other person that violates the CCPA. This bill would delay the operative date of the CCPA by an additional year, to January 1, 2021 and make other conforming or technical changes. Specifically, **this bill would:**

- 1) Replace references throughout the CCPA to the “sale” of PI with the “sharing” of PI, as defined. Relatedly, this bill would revise the definition of the term “sell” to, instead, become a definition of the term “share” and would repeal the requirement that it be for monetary or other valuable consideration.
- 2) Revise the CCPA section establishing a consumer’s right to access the categories and specific pieces of information that a business collects from them (Civ. Code Sec. 1798.100) to:
 - Specify that a business that receives a verifiable consumer request (VCR) from a consumer to access PI must promptly disclose and deliver (as opposed to “promptly take steps to disclose and deliver” under the CCPA), free of charge to the consumer, the PI required by the section establishing the consumer’s right to access their PI.
 - Delete the ability of the business to deliver a consumer’s PI by mail and further revise the manner in which the information must be provided electronically.
 - Clarify that a business is not required to retain any PI collected for a single, one-time transaction, if such information is not shared, sold, or retained by the business, or to reidentify or otherwise link information that is “not maintained as PI” (as opposed to “not maintained in a manner that would be considered PI,” under the CCPA).

- 3) Add a new provision to the CCPA to require a business to limit its collection of a consumer's PI and sharing of that information with third parties only: (a) as reasonably necessary to provide a service or conduct an activity that a consumer has requested, (b) as reasonably necessary for security or fraud prevention, or (c) as required to comply with a court-issued subpoena, warrant, or order. This bill would also add that a business that collects a consumer's PI must limit its use and retention of PI to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested or a directly related business purpose, provided, however, that PI collected or retained solely for security or fraud prevention shall not be used for related business purposes.
- 4) Broaden the consumer's right of deletion under the CCPA (Civ. Code Sec. 1798.105) so that a consumer has the right to delete any PI *about* the consumer (as opposed to any PI about the consumer which the business has collected *from* the consumer under the CCPA).
- 5) Narrow the right of deletion exceptions so that a business or service provider may only "delay compliance" for a consumer's request to delete the consumer's PI for "so long as it is reasonably necessary" for them to maintain the consumer's PI in order to:
 - Complete the transaction for which the PI was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or 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.
 - Exercise free speech and ensure the right of another consumer to exercise that consumer's right of free speech.
 - Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest, as specified.
- 6) Repeal various other existing exceptions to the CCPA's right to delete. Specifically, this bill would remove the authority for a business or service provider to decline to comply with a consumer's deletion request when necessary in order for the business or service provider to:
 - Comply with the California Electronic Communications Privacy Act.
 - Exercise free speech, ensure the right of another consumer to exercise his or her free speech, or exercise another right provided for by law.
 - Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.
 - Comply with a legal obligation.
 - Otherwise use the consumer's PI, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

- 7) Revise the CCPA’s section establishing the consumer’s right to know what PI a business collects about the consumer (Civ. Code Sec. 1798.110) to:
- Additionally require a business to disclose the specific third parties with whom the business shares PI, and not just the categories of third parties as required by the CCPA.
 - Repeal the CCPA’s provision prohibiting a third party from selling PI about a consumer that has been sold to the third party by a business, unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out, as specified.
- 8) Revise the CCPA section establishing the rights of consumers to “opt-out” or “opt-in” to the sale of their PI depending on the consumer’s age (Civ. Code Sec. 1798.120) to, instead:
- Specify that a business shall not share a consumer’s PI unless the consumer has affirmatively authorized the sharing, which is otherwise known as the right to “opt-in.”
 - Require a business to request a user’s opt-in consent separately from any other permission or consent, with the option to decline consent at least as prominent as the option to provide consent.
 - Provide that if a consumer declines to provide their opt-in consent, the business must refrain for at least 12 months before again requesting that the consumer provide their opt-in consent (consistent with a requirement already in the CCPA). The business may, however, make available a setting or other user control that the consumer may affirmatively access in order to consent to additional data sharing.
 - Provide that a business that obtains a consumer’s opt-in consent to share their PI pursuant to these provisions must provide consumers the ability to withdraw such consent through a readily usable and automated means at any time.
 - Require that a business use any PI in connection with the withdrawal of opt-in consent solely for the purposes of complying with the request.
 - Specify that if the business has actual knowledge that the consumer is less than 13 years of age, the consumer’s parent or guardian must affirmatively authorize the sharing of the consumer’s PI.
- 9) Repeal, within the CCPA’s “non-discrimination” section securing the consumer’s right to equal service and price (Civ. Code Sec. 1798.125), authorization for a business to offer certain financial incentives that are not unjust, unreasonable, coercive, or usurious, as specified.
- 10) Revise the CCPA’s section defining various terms for the act (Civ. Code Sec. 1798.140) to:
- Rename the “aggregate consumer information” definition to “aggregate information.”
 - Modify the “biometric information” definition as well as the “research” definition.
 - Revise the “business purposes” definition to, instead, generally mean the use of PI when reasonably necessary and proportionate to achieve one of various enumerated purposes.

- Revise the “deidentified” definition to include an additional condition, wherein the business using the deidentified information must also take “reasonable measures to ensure that the data is deidentified.”
 - Revise the “PI” definition to expressly include information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular device. This bill would further clarify what “publicly available” means for purposes of the PI definition and would correct a drafting error in the definition to state that “PI” does not include PI that is deidentified or aggregated.
 - Narrow the CCPA exemptions from the definition of “sell,” hereinafter to be the exemptions from the definition of “share.” Specifically, it would remove the provision that states a business does not sell PI when a consumer uses or directs the business to intentionally disclose PI or uses the business to intentionally interact, as specified, with a third party, provided that the third party does not also sell the PI, unless that disclosure would be consistent with the provisions of this title.
 - Repeal the “pseudonymize or pseudonymization” definition.
- 11) Amend several exemptions under the CCPA (Civ. Code Sec. 1798.145) to, among other things, state that the obligations imposed on businesses by the act shall not restrict a business’s ability to:
- Comply with the requirements of federal, state, or local laws, or regulations (as opposed to “comply with federal, state, or local laws” under the CCPA).
 - Comply with a court-issued subpoena, warrant, or order.
 - Share information if (a) the business, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires sharing of the information; or (b) the information is shared with the National Center for Missing and Exploited Children in connection with a report submitted pursuant to federal law.
- 12) Create expanded liability of a business for the acts of a service provider, as specified. Specifically, the business must also make reasonable efforts to ensure compliance with the CCPA by the service provider.
- 13) Provide that a service provider shall not be liable for violations of the CCPA by the business for which it provides services as set forth in the CCPA, including by the failure of the business to notify the service provider of a deletion request, as otherwise required.
- 14) Expand the CCPA’s public enforcement mechanism (Civ. Code Sec. 1798.155) by authorizing a county district attorney, a city attorney, or a county counsel to also bring a civil action, in the name of the of the people of the State of California, against any business, service provider, or other person that violates the CCPA (whereas the CCPA only authorizes the AG to bring such actions).

- 15) Repeal the provision of the CCPA authorizing a business to seek the opinion of the AG for guidance on how to comply with the provisions of the act and repeal any ability for businesses' to cure violations upon notice of alleged noncompliance.
- 16) Repeal the CCPA's section stating its intent to supplement federal and state law, as specified.
- 17) Include a severability clause.
- 18) Delay the operative date of the act and the deadline for the AG's regulations to January 1 and July 1, 2021, respectively.
- 19) Codify the CCPA's findings and declarations with certain modifications *emphasized* below, including the CCPA's stated intent of the Legislature to further Californians' right to privacy by giving consumers an effective way to control their PI, by ensuring the following rights:
 - The right of Californians to know what PI is being collected about them *and how it is used*.
 - The right of Californians to know whether their PI is sold or disclosed and to whom.
 - The right of Californians to say no to the sale *or sharing* of PI.
 - The right of Californians to access their PI.
 - The right of Californians to equal service and price, even if they exercise their privacy rights.
- 20) Make other conforming or otherwise technical changes throughout the CCPA.

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:
- 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.
 - Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.
 - Comply with the California Electronic Communications Privacy Act, as specified.
 - Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses’ deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.
 - Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer’s relationship with the business.
 - Comply with a legal obligation.
 - Otherwise use the consumer’s PI, internally, in a lawful manner that is compatible with the context in which the consumer provided the information. (Civ. Code Sec. 1798.105, “the right to delete.”)
- 4) Provides, specifically, that consumers have the right to request that a business that *collects* PI about the consumer disclose to the consumer the following (and requires that the business disclose, as specified below, such information upon receipt of a VCR):

- The categories of PI it has collected about that consumer.
 - The categories of sources from which the PI is collected.
 - The business or commercial purpose for collecting or selling PI.
 - The categories of third parties with whom the business shares PI.
 - The specific pieces of PI it has collected about that consumer. (Civ. Code Sec. 1798.110; “the right to know what PI a business collects about the consumer.”)
- 5) Provides, specifically, that consumers have the right to request that a business that *sells* the consumer’s PI, or that discloses it for a business purpose, disclose to that consumer the following (and requires that the business disclose, as specified below, such information upon receipt of a VCR):
- The categories of PI that the business collected about the consumer.
 - 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 categories of PI that the business disclosed about the consumer for a business purpose. (Civ. Code Sec. 1798.115; “the right to know what PI a business sells about the consumer.”)
- 6) 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.) Requires a business, for a consumer who has opted-out of the sale of the consumer’s PI, to respect the consumer’s decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer’s PI. (Civ. Code Sec. 1798.135.)
- 7) Prohibits a business from discriminating against a consumer because the consumer exercised any of the consumer’s rights under the CCPA, including, but not limited to, by:
- Denying goods or services to the consumer.
 - Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
 - Providing a different level or quality of goods or services to the consumer.
 - Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services. (Civ. Code Sec. 1798.125(a)(1), “the right to equal service and price.”)

- 8) Specifies that nothing in the CCPA's anti-discrimination statute prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data. (Civ. Code Sec. 1798.125(a)(2).)
- 9) Expressly authorizes a business to offer financial incentives, including payments to consumers as compensation, for the collection of PI, the sale of PI, or the deletion of PI. Further authorizes a business to offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data. (Civ. Code Sec. 1798.125(b)(1).)
- 10) Requires a business that offers any such financial incentives to notify consumers of the financial incentive, as specified, and authorizes a business to enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent, as specified, which clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time. (Civ. Code Sec. 1798.125(b)(2)-(3).)
- 11) Prohibits a business from using financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature. (Civ. Code Sec. 1798.125(b)(4).)
- 12) Provides various exemptions under the CCPA. Of relevance to this bill, specifies 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.)
- 13) Provides a limited private right of action for the CCPA's data breach section, as specified, and otherwise provides for enforcement of the act by the AG. Permits businesses to seek the opinion of the AG for guidance on how to comply with the CCPA. Includes a right to cure for businesses, if possible, as specified. (Civ. Code Secs. 1798.150 and 1798.155.)
- 14) Provides various definitions under the CCPA. The CCPA, of particular relevance for this bill, defines the following terms:
 - "Business purpose" means the use of PI for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of PI shall be reasonably necessary and proportionate to achieve the operational purpose for which the PI was collected or processed or for another operational purpose that is compatible with the context in which the PI was collected. Business purposes are, among other things:

- Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.
- Short-term, transient use, provided the PI that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.
- Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.
- “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.
- “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 specific types of information if it 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, 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.

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.

- "Pseudonymize" or "Pseudonymization" means the processing of PI in a manner that renders the PI no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the PI is not attributed to an identified or identifiable consumer.
- "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 act.
 - 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: Unknown

COMMENTS:

- 1) **Purpose of this bill:** This bill seeks to reconsider many elements of the recently enacted CCPA to revise and include additional consumer rights. This bill is co-sponsored by American Civil Liberties Union of California, Electronic Frontier Foundation, and Privacy Rights Clearinghouse.

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

Th[is] bill will build on the protections of the CCPA by prohibiting a business from sharing a consumer's personal information unless the consumer has authorized that sharing and would prescribe various business requirements in connection with this new "right to opt-in consent." In addition, this bill would also prohibit any discrimination against a consumer based on the exercise of the right to opt-in or other rights, including charging different prices for goods or services and require a business that collects personal information to limit its use and retention of personal information to what is reasonably necessary to provide a service or conduct an activity, as specified, subject to certain exceptions. The bill would broaden the duties of businesses regarding requirements connected with disclosure, access, and deletion of consumer information and redefine "business purpose," "personal information," "sell," "research," and other terms. Additionally, the bill would eliminate certain exceptions to the obligations imposed on a business in connection with its provisions.

This bill would also expand the enforcement provisions currently granted to the Attorney General to apply to county district attorneys and city attorneys, among others, and would eliminate the opportunity of a business to cure a violation within 30 days. It would also provide that the California Consumer Privacy Act of 2018 would be operative January 1, 2021, and revise the preemption of local rules and regulations currently in effect as of that date to apply to provisions that are in conflict with the act.

3) **CCPA background:** Last year, the 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 CCPA was the byproduct of compromises made between business interests 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.

The compromise is evidenced by how the CCPA incorporates increased consumer rights (such as the right of deletion, right to specific pieces of information, and the separate treatment of minors' data through an "opt-in" right) that would not have been in the underlying ballot initiative that served as the impetus and starting point for the final legislation. It is further evidenced by how, in turn, certain items were not included in (such as a whistleblower provision), limited by (such as the private right of action, and a single public enforcement entity as opposed to enforcement by all public prosecutors), or added to (such as the authorization for businesses to seek guidance from the AG) the CCPA to alleviate certain concerns that businesses had with respect to the ballot initiative.

This bill would substantially alter, if not eliminate, key tenets of that compromise, including, among other things a business's right to cure, ability to seek guidance from the AG on how to comply with the law, ability to provide some nondiscriminatory financial incentives to consumers, and the obligation to provide consumers the categories (as opposed to specific) third parties to whom the consumer's PI was collected and shared with or sold to or disclosed for a business purpose. At the same time, it would expand various rights that were granted to consumers, such as the right of certain minors to "opt-in" separate and apart from their

parents, and the right of deletion. While one legislature may not legally bind the future acts of another, arguably, the ink on the CCPA has not yet dried and returning members who negotiated and approved the agreement in good faith now face a decision of whether or not to undermine the agreement they supported before it even takes effect (January 1, 2020). Stated another way, while it might be legally permissible for a legislative body to undo the acts of another from one year to the next, it may not be the most desirable. As a matter of public policy, such a significant shift in the law just months after the enactment of landmark legislation can create uncertainty in the judgment of the Legislature and, arguably, may disrupt both consumer confidence and business trust.

a) Tradeoffs made to increase consumer rights and protections in AB 375

As stated in this Committee's analysis of AB 375 at the time it heard the bill last year, certain changes were made to the initiative, to increase consumer rights and protections:

[...] In contrast to the initiative, which includes many but not all of those same rights, this bill enhances various consumer rights and protections, by, among other things:

- Ensuring that consumers can access the PI that business collects about them, not just in terms of the categories of PI collected, but also with respect to the specific pieces of PI that the business has collected. Moreover, if this information is provided electronically, AB 375 ensures that the information must be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance.
- Establishing the right of consumers to request the deletion of the PI that a business has collected from the consumer (as opposed to from other consumers, in order to protect First Amendment rights of those other consumers), subject to certain exceptions.
- Expanding the right of consumers to know what PI a business has collected about them to include the ability to find out not just the categories of PI collected, but also the *specific pieces* of PI that the business has collected about that consumer. Moreover, AB 375 grants the consumer a right to know the *sources* from which the PI is collected, as well as the *business or commercial purpose* for collecting or selling the PI.
- Addressing the PI of children separately from that of parents or guardians, as opposed to classifying all children's information as a subcategory of the parent's PI.

In addition to these items, AB 375's provisions differ from the initiative measure by addressing the recent Cambridge Analytica situation head on (wherein the PI of at least 87 million Facebook users was harvested and used by a "third party" in an effort to influence the 2016 U.S. presidential election), and clearly prohibiting third parties from further selling or disclosing information received from a business unless the third party complies with the provisions of this bill.

Staff notes that yet another significant difference between this bill and the initiative is that the "publicly available" exception to PI in this bill excludes language from the

initiative which states that publicly available information (and thus, *not* “PI” under the initiative) is information that is “available to the general public.” This difference should remove any doubt that information about individuals, and particularly younger generations, that is not privately held, whether by that individual’s choice or not (*e.g.*, information found on a person’s social media posts or the posts of their friends) is not “publicly available” and, thus, exempt from the definition of PI. To exclude such information from the definition of PI could have significant unintended consequences and could very well result in litigation to determine whether or not certain information is “available to the general public” or not. (*See* Asm. Privacy and Consumer Protection Com., analysis of AB 375 (2017-2018 Reg. Session), Jun. 27, 2018, p. 15.)

b) Tradeoffs made to address business concerns

The analysis of AB 375 then turned to the compromises made to address business concerns, as follows:

As discussed [...] above, in order to reach a legislative compromise on the issues surrounding the collection and sale of a consumer’s PI by a business, the authors of this legislation have sought to both add protections to the initiative, and remove various provisions that raised workability issues/legitimate business practice concerns and otherwise limit liability exposure. The tradeoffs to address industry concerns and counterbalance the consumer rights added within this bill, include the following:

- the removal of the initiative’s whistleblower provisions;
- a significant reduction of business’ liability exposure pursuant to consumer-initiated actions;
- a right to cure, when possible, both in the public and private enforcement provisions;
- a limitation of public enforcement to actions by the AG and explicit authorization to receive guidance from the AG on compliance as the single regulatory entity;
- a recognition of the ability of businesses to engage in various research-related activities, such for internal research and development, or other allowable forms of research with specified safeguards that would both ensure informed consent and better protect the consumers’ information used in the research;
- additional express exemptions, such as to exercise or defend legal claims, or for PI collected, processed, sold, or disclosed pursuant to certain federal laws, if the handling of the PI is in conflict with that those laws.
- language clarifying that businesses are not required to retain PI in situations where they would not ordinarily maintain that information (which would also undermine consumer protections);
- authorization to engage in certain financial incentive programs, as specified, such as free subscription services in exchange for advertising where the value to the consumer is based on the consumer’s data, as long as the financial incentive program

is not unjust, unreasonable, coercive, or usurious and is directly related to the value provided to the consumer by the consumer's data;

- a narrowing of the definition of "sell" to remove reference to situations that do not involve valuable consideration; and
- [a limitation on] the obligation of businesses to reveal to consumers to whom the consumer's PI was collected and shared with, or sold to or disclosed for a business purpose to, to "categories" of third parties, as opposed to specific third parties.

With respect to enforcement specifically, [AB 375] would create a limited private right action for consumers whose information is subject to specified data breaches, and would otherwise generally provide for enforcement of the rights and obligations of the bill by way of public enforcement by the AG. This limitation on the private right of action, however, does not relieve any parties from their duties and obligations under any other law or the constitution. As indicated above, the bill would also recognize the ability of businesses to seek guidance from the AG about how to comply with the provisions of this bill, to ensure a single enforcement/regulatory entity. To that end, the AG would also be charged with adopting regulations in furtherance of this bill. These regulations would include, among other things, regulations on the financial incentive programs authorized under this bill. (*Id.* at pp. 15-16.)

4) **General comparison to CCPA and impact of a delayed operative date:** This bill seeks to redraft key elements of the CCPA and shift the focus of the act of from the "sale" of a consumer's PI, which the CCPA defines broadly to generally include any form of dissemination for valuable consideration, to the "sharing" of a consumer's PI, as specified, whether it is for valuable consideration or not. This bill also eliminates the CCPA's "single regulator and enforcement entity" construct, by expanding the list of public entities that may bring a civil action against a business that violates the CCPA to include not only the AG, but also county district attorneys, city attorneys, and county counsels. Additionally, as compared to the CCPA's existing rights and obligations, this bill would:

- Replace the right of all consumers' over the age of 16 to opt-out of businesses selling their PI and the right of all consumers under 16 years of age to opt-in before businesses may ever sell their PI, with, instead, a right to opt-in for consumers of all ages before businesses may share their PI.
- Remove any ability for businesses to provide certain financial incentives that are nondiscriminatory, as specified under the CCPA.
- Generally limit the collection, use, and retention of PI by a business to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested, as specified, subject to certain exceptions (drawing on a concept known as "data minimization").
- Broaden the duties of businesses regarding CCPA requirements connected with disclosure, access, and deletion of consumer information, while simultaneously narrowing certain CCPA exemptions (including exemptions that are specific to the consumer's request to delete PI). This includes the right to know which *specific* third

parties the business has shared their information, and not just the categories of third parties.

- Redefine various terms such as “business purpose,” “PI,” “sell,” and “deidentified,” among others, and repeal the CCPA definition of “pseudonymize or pseudonymization.”
- Repeal businesses’ right to cure and their authorization to seek guidance related to compliance from the AG’s office.

Notably, this bill would also delay the January 1, 2020, operative date of the CCPA by an additional year, to January 1, 2021. Arguably, delaying the effectuation of the CCPA’s rights provides additional time for the federal government to act to preempt those rights.

- 5) **Selling versus sharing:** As noted above, this bill seeks to change the terminology in the CCPA to cause many of the rights and obligations of the act to be triggered based upon a covered business “sharing” a consumer’s PI, as opposed to “selling” the consumer’s PI. The current definition of “sale” under the CCPA is intentionally broad, so as to capture any form of dissemination for valuable consideration – which includes, for example, the sharing or swapping of customer lists. As noted in Comment 3, above, adding the requirement of monetary or other valuable consideration was part of the agreement that led to the adoption of the CCPA in AB 375. Under this bill, however, the definition of “share” includes selling, but also includes other forms of dissemination, even if it is not for valuable consideration.

As argued by a coalition of business groups led by California Chamber of Commerce (CalChamber), “[w]hile the CCPA requires consumers to opt-out of the sale of data, AB 1760 would require consumers to opt-in to the sharing of data. One of the central goals of CCPA is to provide consumers transparency into what consumer information is sold to third parties. AB 1760 has an entirely different goal by changing the focus on what information is shared. The CCPA already contains a very broad definition of “sell” but AB 1760 would expand this to any information a business shares. This erodes the goal of CCPA to provide meaningful transparency to consumers because consumers would be inundated with a massive quantity of useless information that is disconnected from what is being sold. Any potential marginal increase in consumer benefit is outweighed by a massive detriment to how business is conducted. Changing the CCPA from an opt-out of selling to an opt-in for sharing would create an entirely new law with many consequences that cannot [...] even be predicted at this time.”

- 6) **Opt-in mechanism:** As noted above, under the CCPA, all consumers’ over the age of 16 have the right to opt-out of businesses selling their PI. Also under the CCPA, with respect to minors under 16 years of age, a business is prohibited from selling the PI of a consumer who is at least 13 years of age but under the age of 16, unless the minor opts-in to the sale of their PI. For minors under the age of 13 years, the parent or guardian retains the right to opt-in before businesses may ever sell the minor’s PI. Treating children’s PI separately from the parent’s PI, and obtaining the right to opt-in for children, were key additions made to the law under AB 375, as compared to the initiative.

This bill would now seek to extend the right to opt-in. Specifically, this bill would preclude a business from ever sharing a consumer’s PI, regardless of the consumer’s age, unless the consumer has opted-in. With respect to certain minors, this bill specifies as a standalone provision in the opt-in section that “[i]f the business has actual knowledge that the consumer

is less than 13 years of age, the consumer's parent or guardian shall affirmatively authorize the sharing of the consumer's PI." Presumably, the author and proponents intend for the provision to be read to mean that if the business has actual knowledge that the consumer is less than 13 years of age, the business shall not share the minor's information unless the parent or guardian affirmatively authorizes the sharing of the minor consumer's PI.

A coalition of trade organizations, including the Association of National Advertisers, writes in opposition, particularly with respect to this provision in the bill:

No other privacy legislation being seriously considered in the rest of the country has as broad an opt-in consent requirement as AB 1760. There are multitude reasons why opt-in consent for data processing has never been broadly adopted in the United States and should not be mandated under California law. First, opt-in consent fails consumers, placing the burden on consumers, forcing them to read pages of terms and conditions and endlessly click "I Accept." The constant appearances of consent boxes annoy online users and frustrate the consumer experience. Consumers also become desensitized to the constant requests, diminishing their sense of control over their privacy.

Additionally, opt-in consent will remove significant amounts of innocuous data that is used to serve the targeted advertisements that fuel free and low cost products and services. Without the ability to effectively advertise online due to opt-in consent barriers, revenues will be impacted and companies that rely on such revenue may no longer be able to support free and low cost content and services that Californians desire, such as online newspapers, social networking sites, mobile applications, email, and phone services. As a result, companies will be forced to charge consumers higher prices or create pay-walls that will disproportionately impact less affluent Californians. Opt-in regimes also create major barriers for new companies trying to enter the market as consumers may be reluctant to opt in to companies that are not yet well known to them. This will undermine competition in the marketplace.

The CalChamber coalition writes in opposition:

The CCPA is structured as an opt-out regime for all adult consumers. AB 1760's attempt to write over the CCPA and change it to an opt-in law creates numerous problems. First, consumers would be inundated with requests by businesses asking for opt-ins. The bill also requires businesses to obtain specific opt-in consent separate from any other consent. The requirement to obtain multiple distinct affirmative agreements would create a significant burden on consumers and make them especially numb to the importance of notice and choice. Second, the CCPA was not structured as an opt-in law, so AB 1760's amendments to it do not adequately allow businesses to provide products and services absent an opt-in because that is not what it was written to do. Third, AB 1760 compounds the problems of an opt-in by also striking the provision (in section 1798.125) that recognizes that businesses may need to give different levels of service depending on how much information is shared. [...]

AB 1760 cannot flip a switch and make CCPA an opt-in law without significant ramifications that would unwind the last year of work, the Attorney General's current rule making, and the 2019 conversation currently underway.

- 7) **Data portability:** Under the CCPA, a business that receives a VCR from a consumer to access PI must promptly take steps to disclose and deliver, free of charge to the consumer, the PI required by the section establishing the consumer's right to access their PI. The CCPA provides that the information may be delivered by mail or electronically, and if provided electronically, the information must be in a portable and, to the extent technically feasible, a readily usable format that allows the consumer to transmit this information without hindrance. This bill would, instead, provide that the business must, in that situation, promptly disclose and deliver (as opposed to promptly take steps to disclose and deliver), free of charge to the consumer the required PI. This bill would further state that on a verifiable request to do so from the consumer, the business shall disclose the specific pieces of the consumer's PI in an electronic, portable, machine-readable, and readily usable format or formats, that allow the consumer both to understand this information and to transmit it to another business without hindrance. It is unclear how this provision might affect a consumer that does not have access to a computer. Potentially, it could foreclose such a consumer, as a practical matter, from obtaining access to their own information and having the ability to transmit it in non-electronic based formats for their personal purposes.
- 8) **Introducing the concept of data minimization:** This bill seeks to add a new provision that would require a business that collects a consumer's PI to limit its collection of PI and sharing of that information with third parties only (a) as reasonably necessary to provide a service or conduct an activity that a consumer has requested, (b) as reasonably necessary for security or fraud prevention, or (3) as required to comply with a court-issued subpoena, warrant, or order. It also adds, under this new provision, that a business that collects a consumer's PI must limit its use and retention of PI to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested or a directly related business purpose, provided, however, that PI collected or retained solely for security or fraud prevention shall not be used for related business purposes.
- 9) **Changes to right of deletion and First Amendment concerns:** Under the CCPA, any consumer has the right to delete any PI about themselves that the business has collected *from* the consumer. This framework protects the First Amendment rights of others. For example, the First Amendment protects the dissemination of publicly available information. Under this bill, however, if a business were to collect information about a consumer from a public record, the consumer could require them to delete that information, even though it would arguably interfere with the First Amendment rights of that business to have and further disseminate that information. Additionally, the consumer could require that a business delete not only the consumer's photographs from their social media page, but also photographs of the consumer from other consumers' social media pages – which could interfere with the other consumers' First Amendment rights.

In an apparent effort to address First Amendment concerns, this bill provides that a business or service provider “may delay compliance” with the consumer's request “for so long as it is reasonably necessary” for the business or service provider to maintain the consumer's PI in order to exercise free speech and ensure the right of another consumer to exercise that consumer's right of speech.

- 10) **Role of the Attorney General:** Under the CCPA, there is to be a “single regulator/enforcer” (the AG) to ensure that there will be consistent application of the law, from city to city, county by county. The CCPA also allows businesses to seek guidance from that entity, to

ensure compliance with its provisions. This bill would not only allow other public prosecutors to bring civil actions against businesses that violate the CCPA, but it removes any authorization for businesses to seek guidance. The bill also removes the ability of businesses to cure alleged violations. All of these elements were critical components of the agreement reached on the CCPA on that law's enforcement structure. (*See* Comment 3.)

Notably, the CCPA does not require that the AG provide any particular form of guidance, or require that the AG provide any guidance in a binding manner; it merely allows businesses to seek whatever guidance the AG is willing to provide. At minimum, it is unclear why this bill seeks to remove authorization for businesses to seek guidance from the AG on how to comply with the law. Presumably, such guidance could help avoid violations of consumers' rights. Additionally, the CalChamber coalition takes particular exception with the removal of the AG as the regulator of the CCPA.

The CCPA was largely modeled after the European Union's General Data Protection Regulation (GDPR), a law that is enforced by regulators who can offer guidance, issue warnings, and impose fines. California, too, needs a regulator for the CCPA to work, and the Legislature selected the Attorney General to fill that role for two main reasons: (1) the Attorney General's office already has a team of privacy experts – their Privacy Enforcement and Protection Unit has achieved significant results and headlines since their inception in 2012; and (2) the Attorney General's office already has the infrastructure in place to ensure that this complex law and its regulations are enforced uniformly throughout the state.

AB 1760 doesn't just remove the Attorney General as the regulator of the CCPA – it removes the role of any regulator. AB 1760 rolls back businesses' right to seek guidance from a regulator as well as their right to cure in case their good faith efforts to comply with the many nuances of the CCPA fall short. This law applies to businesses of all sizes across every industry – and this includes small businesses – that are going to be genuinely overwhelmed by the complexity and the magnitude of the CCPA.

AB 1760's addition of district attorneys, city attorneys, and county counsel from across California as new enforcers of the CCPA will only create more complexity and confusion in the implementation of this new law. Privacy experts disagree over the meaning of certain provisions in the CCPA. For so many of the provisions in the CCPA that require interpretation and decision making by businesses, there is no moral right or wrong answer, there is no precedent for them to look to – the right approach is what the regulator says is the right approach. Thus, the most crucial component of enforcement for the CCPA is uniformity. To open this law up to different interpretations of what constitutes a violation in different parts of the state, or even from different enforcement offices within the same city, would be disastrous.

In support, Consumer Reports writes that “the CCPA currently lacks sufficient enforcement to ensure that it is truly meaningful for consumer privacy. We are particularly troubled by the ‘right to cure’ provision included in the legislation which, depending on how it is interpreted, may enable a business to evade all liability for behavior proscribed by the statute if it remedies its behavior within 30 days of receiving notice of noncompliance. Under this provision, a company might be able to flagrantly violate the law, and only cease its behavior once its privacy-invasive practices were discovered. Companies should not have to receive

legal notice from the Attorney General before being legally responsible for following the law. We appreciate that AB 1760 would remove this provision from the CCPA.”

- 11) **Third party sale of PI:** It is also unclear why this bill would repeal the CCPA provision that prohibits a third party from selling PI about a consumer that has been sold to the third party by a business, unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out, as specified. (*See Comment 3 for more on the intent of this provision to grant greater consumer protections than existed in the initiative.*)
- 12) **Arguments in support:** In support, a coalition of for-profit businesses, including DuckDuckGo, Inc. among others, writes:

We are a broad coalition of for-profit companies that share that privacy commitment and support the CCPA. All of us have California customers and we are currently subject to CCPA’s requirements or may be subject to them in the foreseeable future. As companies that put user privacy at the core of our products and services, we also support legislation that builds on CCPA’s foundation. Our relationship with our users is built on trust—trust that the data they provide to us and other companies will be used only in the ways they understand and expect.

A.B. 1760 holds all covered companies to that standard and makes sure that Californians’ information is protected by default. It will give all Californians the knowledge and power to truly control their personal information, as well as the ability to practically exercise and legally enforce their privacy rights, all without being punished with higher prices or degraded service.

Also in support, Consumer Reports writes:

Consumers want more, not fewer, protections. For example, 92 percent of consumers think that their Internet Service Providers should provide greater control over the sale of their personal information. More than half of consumers don’t trust social media companies to keep their information safely protected. Recent scandals involving the illicit sharing or sale of personal information without consent, such as the Facebook-Cambridge Analytica incident, and reports of unauthorized sharing of location data, for example by the Weather Channel app, have revealed broad unease about data sharing. Clearly, consumers value their devices, connected products, and other apps and services, but they don’t have the confidence that their information is protected.

Consumer Reports appreciates that the CCPA advances consumer protections in several ways. [...] But in many ways, the CCPA does not fully protect consumer privacy, and AB 1760 would further its privacy goals. The CCPA puts a lot of the responsibility on people to figure out every company that collects information about them and opt out—which likely will be too burdensome for many, if not most, consumers. Instead, privacy should be ensured by default. Consumers need data minimization—meaning data collection that is reasonably necessary to operate the service requested by the consumer, in addition to greater control over data sharing, and access to specific pieces of information sold to third parties and the specific third parties to whom it was sold—which is included in this bill. [...]

Consumer Reports also supports this bill because it would remove problematic language in the CCPA that allows companies to charge consumers more for declining to sell their information to third parties. We support true loyalty programs, which the CCPA enables. True loyalty programs simply keep track of customer purchasing in order to incentivize repeat business. Unfortunately, the CCPA goes even further to allow companies to offer financial incentives for the sale of personal information to third parties. More exploitative programs could provide discounts in exchange for building a profile for targeting offers, or could sell information about customer habits to third-party data brokers. The CCPA explicitly states that companies can charge higher prices to consumers who limit access to their data and can offer financial incentives to consumers for the collection and sale of their personal information. This language was added to the CCPA over objections from advocates, who argued that consumers should not be penalized for exercising their privacy rights. That behavior does nothing to reward consumer loyalty, and runs counter to what participating consumers would reasonably expect. [...]

- 13) **Arguments in opposition:** The CalChamber coalition writes in opposition that “AB 1760 is not a bill that merely amends the CCPA. It seeks a completely new privacy law. Nearly every section of the CCPA is touched by AB 1760 – and the numerous changes it seeks are significant and substantive.” The coalition argues the changes are premature and unnecessary:

The recently-passed CCPA is the most robust privacy law in the country. It provides consumers with the right to know what information a business has about them, the rights to access, delete, and opt out of the sale of that information, and the right to not be discriminated against by a business for exercising those privacy rights.

Despite its importance, the CCPA is a complex law that can be confusing and is in need of legislative fixes and clarifications. Further, businesses covered by the CCPA need time to operationalize it, which will include, among many other things, data mapping (which cannot be fully automated, and requires discussions with each business unit and IT), amending contracts with all service providers (which requires legal advice), updating privacy policies (which also requires legal counsel), setting up and maintaining mechanisms for consumers to make requests for access and deletion, and training personnel. Accordingly, the CCPA, which was signed in June of 2018, has an effective date of January 1, 2020. Further, the Attorney General is in the process of drafting regulations to offer businesses of all sizes and across all industries some guidance on how to comply with this complex law. For this reason, at the end of last year’s session, the CCPA’s enforcement date was extended to July 1, 2020.

Due to these necessarily extended deadlines, we have not yet observed the impact the CCPA will have on our state’s economy. Nor have we determined how much the significant costs incurred by businesses to comply with this complex law will raise prices for consumers in this expensive state. These are crucial factors that need to be weighed by Californians before we add more onerous requirements on top of the CCPA. Yet, before the Legislature and the Attorney General can complete their tasks, and before businesses can finalize their implementation of this new law, AB 1760 seeks to pull the rug out from under the CCPA and replace it with a new framework.

“In sum,” the coalition writes, “these fundamental changes to the structure of the CCPA along with the numerous other substantive changes made by AB 1760 would essentially replace the CCPA, require significant redesign of products and systems, and create a worse consumer experience - all without producing any improvement in privacy for consumers.”

The Nonprofit Alliance writes in opposition because “the bill’s expansion of the [CCPA] exacerbates the current problem of the law’s lack of clarity and confusing scope which results in an increased cost of data – a cost increase that will result in the closure of charities or force them to limit their programmatic missions.” Specifically:

Among other things, AB 1760 (Wicks) creates additional obstacles of workability for the CCPA by requiring an opt-in for consumers and broadens the already expansive definitions and duties contained in law.

By way of background, when the CCPA was being negotiated and drafted last year, legislators exempted nonprofits from the bill.

We are grateful to the Legislature for recognizing the clear intent to exclude nonprofits from the *direct* hit of the costly impact of this legislation, we are nevertheless vulnerable to consequential negative effects if the CCPA is not narrowed and clarified as the law’s current status contains many unnecessarily broad, confusing, and difficult to implement sections and definitions that will drive up the cost of data to the point where nonprofits cannot afford to keep their programmatic missions in place or they may have to close their doors altogether. (Emphasis in original.)

- 14) **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 873 (Irwin) seeks to narrow 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 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.

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

SB 1121 (Dodd, Ch. 735, Stats. 2018) *See* Comment 3. This bill 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.

16) **Double-referral:** This bill is double-referred to the Assembly Judiciary Committee.

REGISTERED SUPPORT / OPPOSITION:

Support

American Civil Liberties Union of California (co-sponsor)
Electronic Frontier Foundation (co-sponsor)
Privacy Rights Clearinghouse (co-sponsor)
Bit Chute Limited
Brave Software Inc.
Conva Ventures Inc. aka Fathom Analytics
Disconnect, Inc.
Discourse, aka Civilized Discourse Construction Kit, Inc.
DuckDuckGo, Inc.
Ecosia GmbH
Fastmail Pty Ltd
Fastmail US LLC
Lavabit LLC
Mailr Tech LLP
Mycroft AI Inc.
Nextcloud GmbH
Proton Technologies AG
Purism, SPC
Shiny Frog Limited, aka Bear
Sgrouples, Inc. dba "MeWe"

Snips SAS
Tresorit AG
Tutao GmbH aka Tutanota
Virtru Corp.
Vivaldi Technologies LLC
Whaller SAS

Opposition

American Advertising Federation
American Association of Advertising
Advanced Medical Technology Association (Advamed)
Association of National Advertisers
California Asian Pacific Chamber of Commerce
California Bankers Association
California Cable & Telecommunications Association
California Chamber Of Commerce
California Financial Services Association
California Grocers Association
California Land Title Association
California Restaurant Association
California Retailers Association
Card Coalition
Computing Technology Industry Association
Consumer Data Industry Association
Email Sender and Provider Coalition
Entertainment Software Association
Insights Association
Interactive Advertising Bureau
Internet Association
Network Advertising Initiative
Nonprofit Alliance
Securities Industry and Financial Markets Association
Silicon Valley Leadership Group
State Privacy and Security Coalition, Inc.
Technet

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