Attachment #8

California Coalition, 8/6/18 letter

August 6, 2018

The Honorable Bill Dodd
California State Senate
State Capitol, Room 5064
Sacramento, CA 95814

SUBJECT: SB 1121 (DODD) – BUSINESS COMMUNITY REQUESTS TO BE INCLUDED IN AB 375 CLEAN-UP LEGISLATION

Dear Senator Dodd:

The undersigned appreciate the work by you and your co-authors on passing AB 375 to secure the removal of the privacy initiative from the November 2018 ballot. We agree that the Legislature is a better venue for debating data privacy issues than the ballot box.

We are grateful for your recognition of the shortcomings of AB 375, the need for some immediate clean-up, and your commitment to a deeper evaluation of the broader issues with this legislation starting in the fall. We appreciate your making SB 1121 available as a vehicle for clean-up this August.

While the full implications of the hastily passed AB 375 are far from being fully understood, in this letter, we propose amendments to address drafting errors, and to fix aspects of this bill that would be unworkable and that would result in negative consequences unintended by the authors.

It is important to fix as many of these problems as soon as possible. The stakes are too high to delay any further – for consumers, businesses, the Attorney General, and the economy.

As the many negative, unintended impacts of AB 375 are more fully understood in the coming months, we look forward to working with the Legislature on the broader issues and, accordingly, on legislation separate from SB 1121 to address those matters next year.

Concerns Regarding Implementation

(1) Delay Implementation of AB 375 to 12-Months After Completion of Attorney General's Rulemaking Process

Our most immediate concern is with the timing of the Attorney General's rulemaking process. Despite the fact that the rulemaking process will provide key inputs and interpretations to many of the statutory requirements, we do not yet know when the Attorney General will have the resources necessary to complete the robust rulemaking process directed by AB 375. And, with a full legislative year before us in 2019, it would be prudent to allow the legislature's statutory work to conclude prior to the beginning of any rule making. Moreover, it does not make sense to require businesses to comply with the provisions of AB 375 until a reasonable time after the AG's regulations have been completed.

AB 375 imposes complex operational requirements that place a massive burden on companies to become ready for compliance. For example, businesses must for the first time track, delete, and provide access to huge volumes of IP addresses both for consumers and seemingly also for industrial devices. These and many more very specific requirements are new – many differing even from Europe's GDPR - and require significant operational and technological changes.

Many businesses will need to incur significant resources for outside experts and operational consultants to help them determine the changes necessary to their specific business to comply with AB 375. Businesses will, in many cases, also need to expend significant time and resources to map data flows, conduct data inventories geared to AB 375's unique definition of "personal information," deploy technology controls, make significant changes to policies and procedures across their businesses, train employees, renegotiate vendor agreements, implement change management controls, and begin processes for monitoring compliance. This sort of effort requires time to come into compliance and businesses cannot be expected to comply if rules are not finalized well in advance of the effective date, much less to incur this cost and effort twice.

Also, due to its broad scope, the statute applies to businesses large and small in almost every industry. For example, the definition of "personal information" includes IP addresses. As such, this bill ostensibly applies to any business that receives 50,000 IP addresses per year on its website – that's an average of about 137 unique visitors per day. Many small businesses will have to comply with this bill, regardless of their level of technological sophistication or their resources. Many larger businesses have numerous operating systems, some in the hundreds, as well as numerous vendors whose compliance they will need to organize. Many businesses have archaic, legacy operating systems. Many businesses have inherited multiple operating systems in the wake of a merger that are not currently set up to communicate with one another. The bottom line is that all of these different types and sizes of businesses will need to comply with this complex, new law. Our request is that the delayed effective date be meaningful to ensure businesses have the time sufficient to be successful in implementation. We believe this was the authors' intent.

It is also unworkable for the AG's regulatory process to commence before the underlying law upon which those regulations would be based is settled and clear. As you and your co-authors have indicated, there will be further debate and discussion about AB 375 in the fall and potentially further clean-up next session. The AG's regulatory process should not commence without clarity surrounding the statutory framework.

Thus, we request clarification that the regulatory process not commence until January 1, 2020 and that compliance not be required until 12 months after the completion of the AG's rulemaking process.

Proposed Language:

Amend Sec. 1798.198 as follows: 1798.198. (a) Subject to limitation provided in subdivision (b), this title shall be operative on January 1, 2020. Compliance with this title shall not be required until 12 months after the publication of the final regulations issued by the Attorney General pursuant to Section 1798.185.

Amend Sec. 1798.185 as follows: 1798.198. (a) On or ~~before~~ after January 1, 2020, the Attorney General shall solicit broad public participation to adopt regulations to further the purpose of this title, including, but not limited to, the following areas:

(2) Clarify Preemption Language to Avoid Regulations at the Local Level as Intended

Issue: The preemption language needs to be clarified to ensure it has its intended effect. Due to the delayed implementation date, preemption may not take effect before a local privacy ordinance may be passed at the ballot in the fall of 2018, which is contrary to the intent of the authors.

Proposed Language:

1798.180. This title is a matter of statewide concern and supersedes and preempts all rules, regulations, codes, ordinances, policies, contracting practices, and other laws adopted or enforced by a city, county, city and county, municipality, ~~or~~ local agency, special district, regional or other body regarding, or that have the effect of regulating the collection, ~~or~~ sale, use, retention, disclosure or other handling by a business of information about consumers. ~~and sale of consumers' personal information by a business.~~

1798.198. (a) Subject to limitation provided in subdivision (b), Section 1798.180 shall be effective immediately upon adoption of this title, while the remaining provisions of this title shall be operative on January 1, 2020. Compliance with this title shall not be required until 12 months after the publication of the final regulations issued by the Attorney General pursuant to Section 1798.185.

Proposed Amendments

(1) Clarify the Definition of Consumer to Avoid Unintended Consequences, Including Deleting Evidence of Workplace Sexual Harassment and More

Current Definition of Consumer: (g) "Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

Issue: The current definition of "consumer" encompasses all California residents, and without clarification could be read as including employees and those involved in business to business interactions. This is contrary to the law's intent as well as its text, including its very title and its multiple references to "consumer data." It would also be unworkable and have numerous unintended consequences. For example, as drafted, an employee accused of sexual harassment could request that complaints about them be expunged (pursuant to the right to delete, Section 1798.105) from company files. In addition, the operational costs of including employees (past and current), job applicants, and other related individuals who do not have a true "consumer" relationship with the business will be exorbitant, and will require many businesses to create separate processes for these individuals. Further, in the context of business to business interactions, the opportunity to delete or opt-out of the disclosure of business data in a business to business transaction could result in fraud and make it impossible to comply with third party due diligence requirements under anti-corruption, anti-money laundering, export control, and Know Your Customer laws. This would result in a chilling effect on commerce and economic opportunities for businesses based in California, and it would impose millions of dollars in compliance costs on companies that are not handling data in the consumer context.

Our proposed clarified provision would continue to cover information originally obtained in a consumer transaction even if it is held by a credit bureau, data broker, or other businesses. However, it would avoid

the problems of including information obtained in employment and business to business situations while aligning the law with the common understanding of who is a consumer.

Proposed Language: Add the following at the end of the definition of "consumer" in Section .140(g): , to the extent the individual's personal information is obtained as a result of the consumer's purchase or use of a product or service for personal, family, or household purposes. Employees or contractors of a business acting in their role as employee or contractor, as well as commercial or non-residential customers of a business, are not "consumers" for purposes of this title.

Issue: Title 18, Section 17014 makes the clarification that a resident includes anyone outside the state for temporary reasons. The law is unclear about how a consumer is identified. It states that someone is a California consumer "however identified, including by unique identifier." It is unclear *who* is identifying the consumer, though, and whether this involves any knowledge on the part of businesses that they have received California consumer data and are therefore subject to the law's requirements.

We propose clarification that it is "the business" who identifies the consumer for the purposes of this definition. This small clarification prevents strict liability, which would have enormous unintended consequences, while furthering the goals of the law.

Proposed Language: Amend this clause in Section .140(g) as follows: "however identified by the business as such, including ~~by any~~ through a unique identifier."

Complete Proposed Definition of Consumer: "Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified by the business as such, including ~~by any~~ through a unique identifier~~.~~, to the extent the individual's personal information is obtained as a result of the consumer's purchase or use of a product or service for personal, family, or household purposes. Employees or contractors of a business acting in their role as employee or contractor as well as commercial or non-residential customers of a business, are not "consumers" for purposes of this title.

(2) To Avoid Unintended Consequences, such as Stalking by a Domestic Abuser or Violations of Roommates' Privacy, Amend the Definition of "Personal Information" to Ensure it is Consistent with the Notion of an Identifiable Person.

Issue: The definition of personal information should be consistent with the notion of an identifiable person, in line with the Obama Administration FTC's definition of "personal information" – including the limitation in the bill that a company does not have to relink or reidentify information in order to comply. The focus of this key definition should be, as it is in California's Shine the Light and CalOPPA laws and every other privacy law and framework, on information that relates to specific *individuals*. The current definition is so sweeping as to be meaningless. Every piece of data could in theory be randomly "associated with an individual".

Fixes:

- Clarify that personal information is limited to information "linked or reasonably linkable" to a particular consumer, *not* information that *relates to* or *could be associated with* a consumer, which is any and all information and is too broad to be useful in shaping the definition. "Linked or reasonably linkable" is consistent with the FTC's guidance on privacy.
- Remove references to household, devices, and family. As drafted, one member of a household, whether they are an abusive spouse or a roommate, can access personal information about another member of their household. This runs counter to the privacy goals of AB 375. Also, the term "device" needs to be deleted because devices are often shared by several people and are not personally identifying. Further, the term "devices" is defined to cover all devices (including even industrial devices) so that it far overshoots anything that might identify an individual.

- Clarify that the list of examples of personal data in A-K are a non-exhaustive list of information that *may* be personal data, but are not always personal information.
- Remove the definition of "probabilistic identifiers" and reference to "probabilistic identifiers" from the definition of "unique personal identifier," which is used in the definition of "personal information." By definition, probabilistic identifiers are not precise. Businesses would be unable to accurately respond to requests for access or opt out or to verify whether the information they are being asked to disclose actually pertains to the person to whom it would be disclosed. Consequently, it is likely that including probabilistic identifiers (i.e., guesses) would require a business to disclose one individual's personal information to a different individual, in violation of the first individual's privacy.
- Remove reference to inferences and tendencies, which are guesses based on patterns of behavior. In addition to the ambiguity of these terms and the ambiguity of how they would be applied, these terms could apply to insights developed through the use of proprietary algorithms and other AI processes. Allowing inferences and tendencies to be included under the definition of personal information will give consumers access to and deletion rights over insights developed with proprietary tools, which creates the potential for reverse engineering.
- Remove references to Professional or Employment-Related Information, in 1798.140(o)(1)(I). This phrase is written so broadly it could be read to confer rights to employees vis-à-vis their employers with respect to their personnel records, and it is not necessary because all identifiable information will be personal data.
- Clarify the scope of the definition of "personal information" to explicitly exclude deidentified, aggregate, pseudonymized consumer information. Pseudonymized information, like deidentified and aggregate consumer information, cannot readily be identified with a particular individual, and is a privacy enhancing process. In order to make the definition of "personal information" consistent with the notion of an identifiable person, none of these terms should be included in it. The current law, due to a drafting error, fails to exempt even deidentified or aggregate data from the definition of "personal information," instead exempting it from the definition of "publicly available data."

Proposed Language:

(o) (1) "Personal information" 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.~~[1] Personal information ~~includes~~ may include, but is not limited to, the following:

(A) 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.

(B) Any categories of personal information described in subdivision (e) of Section 1798.80.

(C) Characteristics of protected classifications under California or federal law.

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

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, ~~thermal, olfactory,~~ [2]or similar information.

---

[1] The term household is used in three other definitions. We request removing this term from all three: 1798.140(a), (c)(1)(B), and (k).

[2] Unclear how thermal or olfactory data would be collected for commercial purposes (e.g. does olfactory refer to scents a consumer likes to smell or to the consumer's unique scent as an identifier?)

~~(I) Professional or employment-related information.~~

(I)~~(J)~~ Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).

~~(J)(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.~~

(2) "Personal information" does not include aggregate consumer information nor information that is deidentified, pseudonymized, or publicly available ~~information~~...

~~(p) "Probabilistic identifier" means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.~~

(x) "Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer~~, a family, or a device~~[3] ~~that is linked to a consumer or family,~~ over time and across different services, including, but not limited to, ~~a device identifier~~; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; or telephone numbers, or other forms of persistent ~~or probabilistic~~ identifiers ~~that~~ if they can be used to identify a particular consumer. ~~or device. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.~~

Issue: Clarify the definition of publicly available information so it is no longer vague and does not violate First Amendment speech protections. The authors intended a public records exemption and this language should be "cleaned up" to reflect an exemption as it is a feature in privacy statutes throughout the country. Publicly available information is for public use and additional limitations on this could violate First Amendment protections for the use of public records. To say data is not publicly available unless it is used for the purpose for which it was made available in a government record is a big departure, defies the common sense understanding of this term, and is an unintended consequence of the way the exemption is currently drafted.

Proposed Language:
(o)(2) "Personal information" does not include aggregate consumer information nor information that is deidentified, pseudonymized, or publicly available ~~information~~. For these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records~~, if any conditions associated with such information~~, or that is available to the general public. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. ~~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. "Publicly available" does not include consumer information that is deidentified or aggregate consumer information.~~

(3) Clarify Exemption for Deidentified Data

Issue: In AB 375, Section 1798.145(a)(5) addresses deidentified and aggregate information, but it does not expressly cover the ability of a business actually to deidentify and thereby to create that information, which is necessary before businesses can then "collect, use, retain, sell or disclose" it. Also, this section does not currently include pseudonymized data, and the need to do so has been addressed above.

If data has been deidentified, aggregated, or psuedonymized, it is by definition, not reasonably linkable to individuals under the statute's definitions of those terms (See, 1798.140(a), (h), and (r)). The collection, use, retention, sale, and disclosure of information in deidentified or aggregate or pseudonymized form, where it can be used in place of personally identifiable information, is privacy enhancing and beneficial to consumers because it means that the processing of personally identifiable information about them is

[3] We also request removing the term "device" from the following: 1798.140(a), (c)(1)(B), and (k).

reduced. Similarly, businesses that can accomplish their legitimate business purposes through the use of deidentified, pseudonymized, and aggregate information can reduce the amount of personally identifiable information that is subject to potential compromise. Section 1798.145(a)(5) appears to recognize the important benefits of aggregate and deidentified information, but in order for the benefits that these types of information provide to be realized, deidentified or aggregate or pseudonymized data first has to be created. This amendment makes it clear through express language, rather than by implication, that deidentified, pseudonymized, and aggregate data can be created, so that such information is available for businesses to "collect, use, retain, sell or disclose" under the provision.

Proposed Language:

1798.145(a)(5) Create, Ccollect, use, retain, sell, or disclose consumer information that is deidentified, pseudonymized, or in the aggregate consumer information."

(4) Clarify the Definition of "Deidentified" so that it is Attainable and to Ensure AB 375 Has Its Intended Effect

Current "Null Set" Definition of Deidentified: "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 using deidentified information:

(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
(2) Has implemented business processes that specifically prohibit reidentification of the information.
(3) Has implemented business processes to prevent inadvertent release of deidentified information.
(4) Makes no attempt to reidentify the information.

Issue: Under the current definition of "Deidentified," only aggregated data (which has a separate definition) would ever be deidentified and businesses would therefore have no incentive to engage in the pro-privacy step of deidentifying personal data. The current definition hinges on whether information "relates to" or "is capable of being associated with . . . a particular consumer". This is always true of deidentified data, and the term loses all meaning unless it is amended. Moreover, this definition is missing key elements of the widely recognized Federal Trade Commission deidentification definition: commitment not to reidentify data and requiring by contract that third parties who receive the data commit not to re-identify it.

Proposed Language: Modify definition of deidentified to align with the 2012 Obama FTC report definition. Amend Section .140(h) as follows:

(h) "Deidentified" means information that does not reasonably identify, is not reasonably capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that the business makes no attempt to re-identify the information, and takes reasonable technical and administrative measures designed to:

(1) Ensure that the data is deidentified;

(2) Publicly commit to maintain and use the data in a deidentified form;

(3) Ensure that third parties with whom the business shares deidentified data do not re-identify the data.

(5) Clarify that No Provision of the Law Requires Businesses to Collect Additional Information or Retain Personal Information Longer Than They Would in the Ordinary Course of Business.

Issue: AB 375 contains 3 different provisions relating to a business not being required to reidentify or retain information in order to comply with the requirements of the law. All of these are pro-privacy in intent but

they are inconsistent. The provisos in Sections 1798.100(e) and .110(d) are limited to compliance with those sections only and limited only to information collected for a one-time transaction. An exception in 1798.145 applies to all sections of the law but only to reidentification, thus by implication suggesting that more information must be collected in order to comply with the other sections of the bill's tricky requirements related to partially identified data.

Proposed Language:

Consolidate the provisos in Sections 1798.100(e) and .110(d) that a business is not required to re-identify or otherwise link information that is not maintained in a manner that would be considered personal information and that it is not required to collect or store more information in order to comply with the exception in 1798.145. This way it would apply to the entire law, and would not be limited to information obtained for a one-time transaction.

Amend Section .145(i) as follows: (i) This title shall not be construed to require a business to collect or retain personal information about a consumer longer than it would be retained in the ordinary course of business or reidentify or otherwise link information that is not maintained in a manner that ~~would be considered personal information~~ identifies an individual.

(6) Remove Requirement that Businesses Should Identify "Specific Pieces of Information" About Consumers

Issue: AB 375 does not explain or define what it means by "specific pieces" of personal information, and providing certain information, such as a consumer's social security number or driver's license number, in response to such requests creates unnecessary risks to both the security of the consumer's information and the business' ability to protect such information. There is also the risk of inadvertent disclosure to a fraudster posing as the consumer. Additionally, to the extent it requires a business to research and re-associate every data element with in the definition of "personal information" with an identifiable individual, it is unworkable.

This change is needed to resolve contradictory sections in the bill, and give effect to exemptions in the bill that clarify a business is not required to relink or reidentify data (see 1798.145, 1798.100, and 1798.110). A business cannot provide "specific pieces of information" without relinking or reidentifying data in order to match it to the person making the request. Indeed, Section 1798.130 already reflects this by directing a business to comply with 1798.110 by identifying "by category or categories" of information.

Requiring a business to maintain records in a form that directly identifies individuals in order to be able to respond to a request for "specific pieces of information" would undermine privacy and these other provisions of AB 375. In order to facilitate Internet commerce while safeguarding consumer privacy and security, businesses typically maintain consumer information in pseudonymized form. This means that information is not directly linked to an identifiable consumer, but it does not necessarily meet the high standard that the FTC has set for information that is "deidentified." Directly linking data contravenes best practices for data security and results in a lower standard of protection for consumer personal information. AB 375 already expands transparency enormously, and this provision is unnecessary from the perspective of increasing transparency and protecting consumers.

Proposed Language:
1798.100(a) – strike reference to "specific pieces"; strike 1798.110(a)(5) and (c)(5) entirely

1798.100(a) A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories ~~and specific pieces~~ of personal information the business has collected.

~~1798.110(a)(5) The specific pieces of personal information it has collected about that consumer.~~

~~1798.110(c)(5) The specific pieces of information the business has collected about that consumer.~~

(7) Clarify the Confusing Language in the Non-Discrimination Section to Preserve Product Features and Fair Discounts for Consumers and Clearly Exempt Loyalty Card and Other Incentive Programs and Data Reasonably Necessary to Provide the Product or Service.

Issue: The exemptions from the law's non-discrimination obligation are inconsistent and confusing. The exemption under (a)(2) includes language about value to the consumer of their own data, rather than the value of the consumer's data to the business offering the service. Moreover, the financial incentives provision creates two inconsistent "reasonably related" and "directly related" standards. Also, there must be an exception for data that is reasonably necessary to provide the product or service. Otherwise, this provision would be impossible to comply with where a user has opted out of data processing necessary to provide them with a particular service or feature, such as where a user opts out of data sharing with a third party that is needed to provide content like music, apps, or games.

These features and programs are typically offered on an opt-in basis, with notice to the consumer that information will be collected and used. These programs are popular with consumers and often provide access to low-cost or free services, such as free WiFi. A confusing set of requirements imposed on such programs could significantly hamper business' ability to offer them and consumers' ability to benefit from them.

Proposed Language:

1798.125

(a) (1) A business shall not unreasonably discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer's rights under this title.

(D) 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.

(2) Nothing in this subdivision 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.

(b) (1) A business may offer ~~financial~~ incentives, including but not limited to, payments to consumers as compensation, for ~~the collection of personal information,~~ the sale or retention of personal information, or the retention ~~deletion~~ of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer, including offering its good or service for no fee, if that price or difference is ~~directly~~reasonably related to the value provided to the ~~consumer~~ business by the consumer's data.

(2) A business that offers any ~~financial~~ incentives pursuant to subdivision (a), shall notify consumers of the ~~financial~~ incentives pursuant to Section 1798.135.

(3) A business may enter a consumer into an ~~financial~~ incentive program only if the consumer gives the business prior opt-in consent ~~pursuant to Section 1798.135~~[4] after notice which clearly describes the material terms of the ~~financial~~ incentive program, and which may be revoked by the consumer at any time.

[4] This cross-reference to the business' "Do Not Sell... "page in 1798.135 doesn't make sense in this context, when the business is offering a consumer the opportunity to enroll in a specific service. The notice and terms of the opt-in consent would be part of the promotion or program enrollment; a consumer would be confused if directed to the Do Not Sell page.

For this purpose, an incentive may also include offering a specific good or service whose functionality is reasonably related to collection, use or sale of the consumer's data. [5]

(4) A business shall not use ~~financial~~ incentive practices that are ~~unjust, unreasonable,~~ coercive[6]~~,~~ or usurious in nature.

(8) Clarify that Selling Targeted Advertising is Not a Sale of "Personal Information" When the Platform is Not Disclosing "Personal Information" to the Ad Purchaser.

Issue: During the process of the privacy initiative and AB 375, many privacy advocates said that it was not their intention to cover targeted advertising as a "sale" where the consumer's identity is not shared. SB 1121 should clarify that the law does not to require an opt out of all advertising. Online advertising allows companies to reach audiences that are likely to be interested in the companies' products or services in a privacy protective way, which does not require the online platform to identify the consumer to the business in order to deliver the business's advertisement. The practice of advertising online in a manner that the advertiser is not able to identify consumers based on that advertising should not unintentionally be restricted by this legislation.

Proposed Language:

1798.140(t)(2):

(E) The business does not share or transfer personal information to another unaffiliated business and the use of the information for advertising for an unaffiliated business does not enable an unaffiliated business to identify a particular consumer.

(9) Allow Consumers the Option to Choose the Types of "Sales" They Want to Opt Out of, Instead of Mandating Only One "All or Nothing" Opt-out

Issue: Currently, AB 375 could be construed to require a business to apply a consumer's opt-out of one type of sale of personal information, such as third-party cookies on a website, to another type of sale, such as a joint marketing email campaign. This could have unintended consequences that harm consumers. For example, if a consumer opts out of receiving online targeted ads resulting from the use of third-party cookies, unless the law is clarified, he or she might also inadvertently be deprived of special discounts and promotions for existing or new services that could save them money. From an operational perspective, it would also require fundamental changes to the existing online self-regulatory, opt-out mechanisms. A prior version of the ballot initiative contained language designed to give consumers these expanded choices, and similar language could be added to Section 1798.120 as follows:

Proposed Language:

(d) A consumer's opt-out request can be limited to specific types of personal information, specific types of sales of personal information, or sales of personal information to categories of third parties. A business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell the minor consumer's personal information shall be prohibited from selling the consumer's personal information unless the consumer subsequently provides affirmative authorization for the sale of the consumer's personal information.

---

[5] Consistent with (a) and (b) above, this clarification reflects that some services need data to work at all. This is a different concept than assigning value to the data. Since "value" isn't defined, this clarification is helpful.

[6] Given the references to reasonableness above, references to unjust and unreasonable are unnecessary here.

(10)Ensure AB 375 Does Not Prevent Protecting Consumers from Crimes of Identity Theft and Other Illegal Activity by Authorizing Data Use for Identity Verification and Fraud Detection Purposes.

Issue: A critical exception for preventing fraud or other criminal activity must be added to Section 1798.145(a)(4) to preserve the effectiveness of anti-fraud, sanctions, and money-laundering screening and identity verification functions and services. To function properly, this exception must provide that a business may sell personal information for this purpose and the other exceptions under 1798.145.

Without these exceptions, AB 375 will jeopardize important efforts to prohibit criminal activities that rely on data supplied by businesses. Criminals will "opt out," which will have downstream effects because these individual will no longer appear in systems provided by vendors that are subject to AB 375 to warn of possible criminal activity. Also, under AB 375, consumers may authorize third parties to opt out of the sale of their information on the consumer's behalf, which would allow a cottage industry to develop offering opt-out services for anti-fraud databases and other identity verification and fraud detection services. The following list demonstrates some of the efforts that would be impacted: anti-terrorism efforts (ensuring people on terrorist watch lists do not have access to financing), anti-money laundering efforts, anti-fraud programs, locating persons of interest in criminal investigations, verification of identities, and officer safety issues, such as the identification of the occupants of an address.

Additionally, once a consumer has "opted out," a criminal will have an easier time fraudulently using the consumer's identity to obtain goods and services, as merchants will no longer be able to use identity verification tools to confirm that the purchaser is who they claim to be.

Without this exception, AB 375 will also undermine government safety-net programs that rely on data supplied by businesses, harming California's most vulnerable populations. Many California government entities utilize data supplied by private companies in fulfilling their mission. If an individual's personal data is unavailable for such use, the effectiveness of the associated government program will suffer. Additionally, increased instances of identity theft caused by AB 375 will undermine the stability of these government programs that rely on identity verification and fraud prevention tools. State and local government programs that would suffer unintended consequences due to the current language of AB 375 include: Medi-Cal (Provider data provided by businesses contracted with the Department of Healthcare Services is used to keep excluded Providers out of the system, protecting citizens); DHCS, DSS, and EDD Program Integrity Divisions; State and County Tax Fraud Prevention and Detection programs; programs ensuring payment of child support (data used to locate non-custodial parents); foster youth programs (data used to connect children with family members, which reduces the number of children in foster care).

Proposed Language:
"(a) The obligations imposed on businesses by this title shall not restrict a business' ability to:

(4) Exercise or defend legal claims, or prevent or detect identity theft, fraud, other criminal activity, or verify identities.
(7) Sell a consumer's personal information for the purpose of assisting another business or a government agency to comply with any of the activities specified in (a)(1)-(6) above.

Alternatively, retain the proposed change in (a)(4) above but instead of adding a new (a)(7) instead put a new section (g):

"(g) This title shall not apply to the sale of personal information for the purpose of assisting another business or a government agency to comply with any of the activities specified in (a)(1)-(6) above."

(11)Ensure AB 375 Does Not Unintentionally Inhibit the ability of Businesses and Government entities to Comply with Federal, state, and local laws.

Issue: 1798.145 (a), the exemption for businesses to comply with federal, state, and local laws, does not address the practical reality that outside entities often provide the data necessary for businesses and

government entities to comply with regulations under federal, state, and local laws, but those vendors do not have the mandate to comply with these regulations themselves. For example, banks and other firms subject to anti-money laundering laws must check customers and potential customers to identify potential Politically Exposed People (PEPs) or individuals on watch lists. Banks cannot try to create and maintain their own accurate sets of PEPs and watch lists. Instead banks comply with their anti-money laundering and PEP obligations by checking lists maintained and constantly updated by outside firms. Similarly, under the FTC Act and other laws, companies that use a vendor to process personal data must conduct due diligence on those vendors (it would be unlawful to accidentally hire a recently convicted identity thief to handle data without doing diligence). In order to undertake such diligence, companies use firms that provide due diligence information about companies and their officers. Similarly, government programs and services often have eligibility and verification requirements that the government entities must comply with before providing funds or services or they will be in violation of federal and state regulations. In these instances, third party contractors often provide the data necessary for staff to authenticate identities, and ensure program integrity within the prescribed rules and regulations.

In these examples, the critical data set is maintained by a vendor rather than by the company or government entity subject to the compliance obligation and the vendor would be subject to the opt-out and disclosure requirements thus defeating the purpose of the compliance exemption.

Proposed Language: 1798.145.

(a) The obligations imposed on businesses by this title shall not restrict a business's ability to:

(1) Comply with federal, state, or local laws~~.~~ nor shall it restrict the ability of a business contracted to collect, use, or provide personal information in order to assist another business or a government agency to comply.

(12)Clarify the scope of GLBA, FCRA, and DPPA Exemptions

GLBA Exemption Clean-Up

Issue: The Gramm-Leach-Bliley Act (GLBA) is a federal law that requires financial institutions to maintain consumer privacy protections and regulates how those institutions may disclose certain consumer information to non-affiliated third parties. Like the FCRA and HIPAA, GLBA is an established and comprehensive federal privacy law that already provides protections for consumers, and should be completely exempt from the requirements imposed by AB 375. There is not a conflict between GLBA and the California law, therefore the current language in AB 375 affords no exemption. For the exemption to function properly, the language needs to be adjusted.

GLBA data is used in fraud prevention and public safety data solutions, therefore the inclusion of this exemption is necessary to ensure the proper functioning of those tools for California public and private entities that rely on this information.

Proposed Language:

(e) This title shall not apply to personal information collected, processed, sold, or disclosed ~~pursuant~~ ***subject*** to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations~~, if it is in conflict with that law~~.

FCRA Exemption Clean-Up

Issue: In 1798.145 (d) the author intends to include a Fair Credit Reporting Act (FCRA) exemption, but it needs to be cleaned up to ensure coverage of legitimate uses of FCRA data. The definition of "sale" was changed between the ballot initiative and AB 375, with the ballot initiative providing that the definition of sale included transactions made for "no consideration" while AB 375 provides there has to be some level of consideration (i.e., money or something of value changing hands). The reason this is important is a concept in the FCRA for "furnishers" which provide information to consumer reporting agencies to be used in consumer reports, sometimes without any form of "consideration." Accordingly, the language for this

section needs to be adjusted to clarify that the entire FCRA ecosystem – including furnishers and all the data provided to, from, or held by a consumer reporting agency that is subject to the FCRA – gets the exemption.

Proposed Language:

> (d) This title shall not apply to ~~the sale of~~ personal information provided to, from, or held by a consumer reporting agency ~~if that information is to be reported in, or used to generate, a consumer report~~ as defined by subdivision ~~(d)~~ (f) of Section 1681a of Title 15 of the United States Code, ~~and use of that information is limited by~~ subject to the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).

DPPA Exemption Clean-Up

Issue: The Driver's Privacy Protection Act (DPPA) is a federal law that regulates the disclosure of personal information from state DMV records and limits the recipients of the records to only those with a permissible purpose, as provided by law. Like the FCRA and HIPAA, DPPA is an established and comprehensive federal privacy law that already provides protections for consumers, and it should be completely exempt from the requirements imposed by AB 375. There is no conflict between DPPA and AB 375, therefore the current language affords no exemption. For the exemption to function properly, the language needs to be adjusted.

The DPPA exemption is crucial for the safety of consumers. Data obtained subject to the DPPA is used to assist automakers in contacting registered owners of vehicles subject to recalls. For example, recent reports indicate that in the Takata airbag recall, there are still over 2.5 million vehicles that have not been repaired in California alone – many with defective airbag inflators that have a high risk of explosion even in a minor accident. Bringing clarity to this exemption will allow those that provide data to automakers the opportunity to assist Californians in this and other auto recalls to help ensure motorist safety and the safety of California roads. DPPA data is also used in support of emissions testing and other safety related matters that benefit all motorists.

The DPPA exemption is also necessary for insurance companies and their support organizations that relay on personal information for purposes of underwriting, claims investigation and resolution, reporting obligations, and other services related to providing insurance. This information, used for permissible purposes under the DPPA, allows insurance carriers to process claims effectively and accurately. If insurance companies are unable to use data from vendors due to limitations on the DPPA exemption and do not have as much personal data to analyze claims, insurers' costs associated with such claims will increase and could be passed down to consumers in the form of higher premiums.

Proposed Language:

> (f) This title shall not apply to personal information collected, processed, sold, or disclosed ~~pursuant~~ subject to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.)~~, if it is in conflict with that act~~.

(13) Clarify the HIPAA Exemption and Ensure that Businesses Will Be Able to Continue to Conduct Life-Saving and Life-Improving Clinical Trials

Issue: In 1798.145(c), the authors clearly intended to include a HIPAA exemption. However, the exemption covers only information "collected by a covered entity," and misses information collected by "business associates." Business associates are defined in HIPAA as service providers to HIPAA-covered health care providers and payers. Business associates are subject to all HIPAA privacy and security obligations. Business associates must be exempt from AB 375 to avoid conflicts with HIPAA requirements, such as differing standards on what constitutes deidentification of data. An example of a business associate (as defined in HIPAA) is a third party administrator (TPA). TPAs contract with health plans and insurers to adjudicate claims — that is, they determine whether the claim is properly filed, which services should be reimbursed, and for how much. If business associates are not exempted from AB 375, insured individuals

could ask that TPAs delete personal information they collect — this would preclude the claim from being processed and the provider would not get paid. Other "business associates" perform administrative, technological, or other services for health plans and health care providers; deleting data from these types of businesses would have a detrimental impact on health care access, payment, and quality in California.

Issue: California is a leader in medical research. Analysis of data associated with the use of new medicines and medical devices in clinical research trials is vital for advancing our ability to diagnose, prevent, and treat diseases and other health conditions. Comprehensive state and federal laws protect the rights of human research subjects, including their right to a detailed understanding of the clinical trial prior to providing informed consent to participate, and their right to privacy of the data collected. Researchers — including pharmaceutical and medical device companies — also adhere to strict protections that have been incorporated into international standards for acceptable clinical research and which are mandated by the U.S. Food and Drug Administration and other federal agencies.

AB 375, as adopted into law, would have the unintended consequence of requiring the deletion of clinical research data in response to the request of a participant. Deletion of clinical research trial data would impair the integrity of the study results, and, for that reason, is prohibited by international standards for Good Clinical Practice and United States Food and Drug Administration guidelines. In addition, AB 375 would give clinical trial participants the right to access data about themselves in blinded clinical trials, even though this would necessitate unblinding (revealing who received which treatment), which would, again, impair study integrity. If state law makes it impossible to conduct a scientifically valid research study and to comply with Good Clinical Practice guidelines and federal research regulations, then federal research dollars and private research grants will not be awarded to California researchers. The state's important biomedical research industry would come to a halt.

Issue: In 1798.145(c), the authors clearly intended to include a HIPAA exemption. This makes sense given HIPAA's strong consumer protections, including the right to a Notice of Privacy Practices, the right to access the medical record, the right to amend incorrect information, the strict prohibitions on disclosures and on sales of information, and other rights. However, the exemption as currently written in AB 375 exempts protected health information (PHI) governed by HIPAA, rather than exempting the businesses that must comply with HIPAA. This means, for example, that hospitals and doctors would have to look at each piece of paper (or electronic file) to determine if the information it contains constitutes PHI or not. If it does, it is exempt from AB 375. If it does not, it is subject to AB 375. To illustrate the problem, consider hospital peer review/disciplinary records. They typically do not contain the name of the patient. However, they may still be considered PHI and thus fall under HIPAA —or they might not. Whether information is considered PHI depends upon whether it can be combined with other available information in a way that would permit the reader to determine the individual patient to whom it pertains. Today, HIPAA covered entities simply treat information that refers to a patient as protected by HIPAA. However, if under AB 375 a consumer can request their information to be deleted, hospitals and doctors would be required to collect all information we held about that individual, and review every bit of it to determine which was protected by HIPAA (and not subject to AB 375 and therefore not required to be deleted) and to determine which was not protected by HIPAA, and thus must be deleted. Under HIPAA, patients already have the right to have their information correct. This new administrative burden — indeed, an administrative nightmare — added by AB 375 would greatly increase the cost of health care without providing any corresponding benefit to the patient.

Proposed Language:

Section 1798.145 (c) shall be amended to read as follows:

(c) (1) This ~~act~~ title shall not apply ~~to~~ to:

(A) ~~protected or health information that is collected by a covered entity~~ "medical information" governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56 of Division 1)) or

"protected health information" that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and ~~Availability~~ Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act of 2009.

(B) a provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with section 56 of Division 1)) or a covered entity governed by the privacy, security, and breach notification rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996.

(C) information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the "Common Rule;" pursuant to Good Clinical Practice guidelines issued by the International Council for Harmonisation; or pursuant to human subject protection requirements of the United States Food and Drug Administration.

(2) For purposes of this subdivision, the definitions of "medical information" and "provider of health care" in Section 56.05 shall apply and the definitions of "business associate," "covered entity" and "protected health information" ~~and "covered entity"~~ from 45 C.F.R. 160.103 ~~the federal privacy rule~~ shall apply.

(14) Ensure AB 375 Does Not Compromise Legitimate Cybersecurity and Crime Prevention Methods

Issue: Several of AB 375's rights create real risk of exposing and undermining company cybersecurity and other security methods. These rights include the rights to: (1) obtain information about the purpose of collecting personal information and about disclosures for business purposes, (2) opt-out of any disclosures for some sort of consideration, and (3) obtain access to specific data held about any state resident. In the specific context of security programs these rights risk that hackers and criminals will obtain critical information about businesses' security programs and any cooperation with law enforcement to prevent crime or share cybersecurity threat information. For this reason, it is very important to create a targeted exemption to protect the confidentiality of these important methods.

Proposed Language: Create a new subdivision 1798.145(k):

"(k) Notwithstanding the rights afforded to consumers and the obligations imposed on businesses under this title, nothing in this Act requires a business to divulge information that the business reasonably believes would jeopardize the security of the business or public safety, including disclosures related to business purposes described in paragraphs 2-3 of subdivision (d) of Section 1798.140."

(15) Clarify that the Standard for Knowledge that a Business has Information of a Minor and Must Request Opt-in Consent is Actual Knowledge, and Eliminate the Confusingly Different Willful Disregard Standard

Issue: The child/teenager privacy provision in the bill appropriately contains an "actual knowledge" standard that the business should have actual knowledge that the user is a child or teenager. This is followed, however, by an inconsistent and confusing sentence that applies a different "willfulness" standard for liability.

Proposed Language: In Section ..120(d)(4) strike the willfulness sentence and leave the actual knowledge sentences to provide a clear legal standard:

(d) Notwithstanding subdivision (a), a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the

sale of the consumer's personal information. ~~A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age.~~

(16)Ensure that a Third Party Will Not Be Liable for Sale of Personal Information Without Having Received Notice of a Consumer's Right to Opt Out

Issue: How would a third party know if a consumer has opted out? The current language of the bill seems to imply strict liability for third parties for opt-outs submitted to another business of which the third party has no knowledge.

Potential fix: Delete the current language in 1798.115(d) and draft the following: "A third party that receives actual notice that a consumer has exercised his or her right to opt-out of the sale of his or her personal information pursuant to 1798.120 shall be bound to comply with that consumer's opt-out and to not sell personal information about the consumer that was sold to the third party by a business."

(17)Clarify that Businesses Have a Reasonable Amount of Time to Implement Opt-Out Requests and Clarify There is No Obligation to Refrain from Asking for Authorization Following an Opt-Out if the Consumer Deletes their Data (Because There Would Be No Way to Screen Them Out) or if the Request is Made by a Different Business Unit.

Issue: If the consumer's data has been deleted, there is no way to prevent inadvertently seeking the consumer's consent because it is impossible to suppress requests for consent when the data have been deleted. In addition, if the consumer exercises his or her right to say "no" to one part of a business, the business must share their information to other business units across the company, which is a net minus for privacy. Also, deleting this would limit the possibility of investigating whether someone had actually opted out, and thereby effectively limiting consumers' rights to opt back in easily.

Proposed Language: Amend Section .135(a)(5) as follows:

For a consumer who has opted out of the sale of the consumer's personal information, respect the consumer's decision to opt out for at least 12 months before the business unit that received the consumer's opt-out direction may requesting that the consumer authorize the sale of the consumer's personal information, unless the consumer has also exercised the right to delete the consumer's personal data.

Issue: Currently, AB 375 does not provide a business with any time to implement a consumer's opt-out request. Executing a consumer's opt-out request may be time consuming because the definition of "personal information" is so broad and difficult to relate to a requester. Language should be added mirroring other laws – such as CAN-SPAM and the Telephone Consumer Protection Act – to accommodate the time it may take for a business to effectuate any opt-out requests.

Proposed Language: Add a new subparagraph to Section 1798.120 that gives businesses time to implement opt-out requests:

(e) A business shall implement a consumer's opt-out request within the timeframe provided by any other applicable law or, if no other applicable law applies, within 45 days and refrain from initiating any sale of a consumer's personal information after that time, unless the consumer subsequently provides affirmative authorization for the sale of such personal information.

(18)Remove Inadvertent Vestiges of Data Portability Mandate Already Deleted from AB 375

Issue: Fortunately, separate provisions regarding data portability previously included in AB 375 were deleted prior to its passage. Proponents of AB 375 have publicly acknowledged that the bill does not have a "data portability/right to have information sent to a third party." However, in two places, AB 375 inadvertently retained vestiges of the prior section on portability – which will be confusing to businesses attempting to comply with this law. A data portability mandate will be impossible for most businesses to achieve operationally, especially given the bill's very broad definition of personal information. Also, given the sensitive information that is included in the broad definition of personal information (e.g., social security

information, financial information, medical information, etc.), this requirement could invite bad actors to focus on such portability as an attractive source for stealing sensitive information and perpetrating identity theft and other frauds on consumers.

Proposed Language:
Remove the inadvertent vestiges of the data portability mandate from the law.
Sections 198.100 (d)

(d) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. ~~The information may be delivered by mail or electronically, and if provided electronically, the information shall 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.~~ A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.

Section 198.130 (a) (2)

(2) Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable request, but this shall not extend the business's duty to disclose and deliver the information within 45 days of receipt of the consumer's request. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12-month period preceding the business's receipt of the verifiable request. ~~and shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance.~~ The business shall not require the consumer to create an account with the business in order to make a verifiable request.

(19)Remove the One-Size-Fits-All Requirement that Businesses Provide a Toll-free Number to Opt-out and Permit Businesses to Specify Designated Contact Methods for Consumer Requests

Issue: The mandate for a toll-free number should be removed. A toll-free number is a significant expense for any company, particularly small companies, and the likelihood that a phone representative may make a mistake is far greater than if a consumer documents the information in a letter or online. This requirement is dated and would preclude a completely automated customer service experience.

Additionally, we seek clarification that, just as a business must provide notice of designated contact methods, the same business can direct consumers to a specific designated contact method for submitting certain types of activities (e.g., opting out of 3d party advertising cookies must be initiated online).

Proposed Language:

Section 1798.130(a) should be amended as follows:

(1) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, ~~at a minimum, a toll-free telephone number, and~~ if the business maintains an Internet Web site, a Web site address.

Section 1798.140 should be amended as follows:

(i) "Designated methods for submitting requests" means a mailing address, email address, Internet Web page, Internet Web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185. A business may assign

specific designated methods for submitting requests related to specific activities (such as a designated online portal or Web page to request an opt-out of the online sale of personal information).

(20)Clarify Definition of "Home Page" So It Does Not Include Every Webpage on a Website

Issue: A drafting error in the definition of "Home Page" defines it as both the home page *as well as* every web page at which a business collects personal information. The result is to require notices *on every single web page where a business collects any personal information, including an IP address*. Read literally, this would require special California right to know notices on every single business web page

Proposed Language: Strike "and" in this definition and insert "or".

(l) "Homepage" means the introductory page of an Internet Web site ~~and~~ or any Internet Web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, "About," "Information," or settings page, and any other location that allows consumers to review the notice required by subdivision (a) of Section 1798.145, including, but not limited to, before downloading the application.

(21)Give the AG's Office Full Discretion to Determine How to Verify Requests by Cutting Language that Precludes Registration

Issue: How do we know if the person requesting data is the consumer? The law needs to be amended to give the AG the ability to determine what information can be requested to verify a request. The law currently categorically prohibits registration for requests. Because of the significant risk of phishing attempts, the law should give the AG's Office discretion about what verification methods make sense and not prejudge that rulemaking. For example, in the case of jointly held accounts, registration is likely essential to avoid providing one accountholder's info to the other customer.

Proposed Language: At the ends of both Sections .130(a)(2) and 135(b)(1), strike the last sentence: "~~The business shall not require the consumer to create an account with the business in order to make a verifiable request.~~"

Proposed Language for Already Agreed-Upon Amendment

(1) Clarify that AB 375's Private Right of Action Only Applies to Section 1798.150

Issue: The authors made it clear throughout the legislative process their intent that AB 375's private right of action only applies to Section 1798.150, which creates additional liability for businesses in the wake of a data breach. However, the current language of the bill is not clear on this point. Additionally, there needs to be clarity that the AG has the exclusive authority to bring actions for violations of the rest of the title.

Proposed Language:

1798.150

(c) A violation of any other section of this title shall not serve as the basis for a private right of action under subdivision (a). Nothing in this act shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.

1798.155.

Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title. Except as provided in Section 1798.150, exclusive authority to enforce this title is granted to the Attorney General through a civil action brought in the name of the people of the State of California.

(2) Correction of Error Made to 1798.150(a) During Drafting Process

Issue: During the fast-paced discussions that occurred in the days after the text of AB 375 was published, an error was made to the language of Section 1798.150(a), which pertains to the liability of a business in the wake of a data breach. Originally, Section 1798.150 was drafted to apply to a consumer whose "nonencrypted and nonredacted" personal information was subjected to a breach. This meant that if information was either encrypted or redacted, then there would be no liability under the section. Among other things, this sort of language was touted as a way to encourage security practices of businesses. Unfortunately, AB 375 now applies to a consumer whose "nonencrypted or nonredacted" information is breached. This means that a company would be liable if the breached information was encrypted, but not also redacted – and vice versa. As drafted, AB 375 undermines the common security practice of encrypting data and is inconsistent with existing California law.

Proposed Language:

1798.150.(a) (1) Any consumer whose nonencrypted ~~or~~ and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

Next Phase

In addition to the issues raised in this letter to fix unworkable aspects of this bill as well as unintended consequences, there are substantive issues we wish to discuss and address this fall and into 2019, including, but not limited to, creating a safe harbor to the data breach liability that would encourage stronger security practices, revising the definition of sale to align with consumer expectations of what it means to sell, and more. Additionally, we believe additional negative, unintended impacts of AB 375 may come to light in the coming months as more and more businesses plan for compliance and realize the impact of this legislation. Again, we look forward to working with the Legislature on these broader issues and, accordingly, on legislation separate from SB 1121 to address those matters next year.

Sincerely,
California Chamber of Commerce SB
Advanced Medical Technology Association
Alliance of Automobile Manufacturers
American Council of Life Insurers
American Insurance Association
Association of California Life & Health Insurance Companies
Association of National Advertisers
California Bankers Association
California Business Properties Association
California Cable & Telecommunications Association
California Community Banking Network
California Credit Union League
California Financial Services Association
California Hospital Association
California Land Title Association
California Life Sciences Association
California Manufacturers & Technology Association
California Mortgage Bankers Association
California Retailers Association
California Trucking Association
Civil Justice Association of California
CompTIA
Consumer Data Industry Association
Consumer Technology Association
CTIA
Delta Dental
Interactive Advertising Bureau
International Pharmaceutical & Medical Privacy Consortium
Internet Association
Internet Coalition
Motion Picture Association of America
National Association of Insurance and Financial Advisors
National Association of Mutual Insurance Companies
National Business Coalition on E-Commerce and Privacy
NetChoice
Pacific Association of Domestic Insurance Companies
Personal Insurance Federation of California
Retail Industry Leaders Association
Securities Industry and Financial Markets Association
Software and Information Industry Association
TechNet
Wine Institute

cc: Tom Dyer, Office of the Governor
The Honorable Bill Dodd
The Honorable Robert Hertzberg
The Honorable Ed Chau
The Honorable Anthony Rendon

SB:ldl