September 6, 2024

The Honorable Gavin Newsom
Governor, State of California
State Capitol
Sacramento, CA 95814

SUBJECT: AB 1949 (WICKS) CALIFORNIA CONSUMER PRIVACY ACT OF 2020: COLLECTION OF PERSONAL INFORMATION OF A CONSUMER LESS THAN 18 YEARS OF AGE REQUEST FOR VETO

Dear Governor Newsom:

The California Chamber of Commerce and undersigned organizations respectfully request that you **VETO AB 1949** (**Wicks**), which would generally prohibit the collection, sharing, sale, use or disclosure of consumer data for anyone under 18 years of age, absent affirmative consent. Our member companies take seriously the privacy of all their consumers, but especially those relating to children. Unfortunately, by requiring that a business obtain affirmative consent prior to collecting, using, or disclosing the personal information (PI) of anyone under the age of 18, **AB 1949** raises significant workability issues, but also has the effect of compelling companies to further impede consumers' right of privacy to ensure compliance. While we appreciate amendments reinstated the actual knowledge standard into Section 1798.120 relating to the selling or sharing of a minor's personal information, we still have concerns with the overall change to an opt-in structure for other provisions relating to the collection, use and disclosure of a minor's PI, even where the information is collected not *from* the minor, but from other sources as well. We also have significant concerns over how the bill undermines what is understood to mean "actual knowledge".

Unfortunately, it is unclear what problem that this bill is seeking to solve for, particularly when Proposition 24 enhanced existing protections by way of data minimization principles and the like. Expanding the CCPA to add new opt-in requirements at the same that other bills seek to address issues around "consent fatigue" (e.g. AB 3048 Lowenthal), without demonstrating any problem with the existing protections will only overcomplicate an already complicated law and create unnecessary compliance burdens for businesses. In doing so, the bill disrupts the careful and deliberate balance struck by the Legislature in passing the California Consumer Privacy Act (CCPA) in 2018 and affirmed by voters in approving Proposition 24 to expand the CCPA in 2020.

AB 1949 fails to appropriately harmonize with the data privacy laws of other jurisdictions and lacks necessary and reasonable limitations which invariably will lead to consent fatigue but industry offered amendments to remove opposition were rejected

Currently, under the CCPA, minors under the age of 16 have an "opt-in right" to the sale or sharing of their PI. In furtherance of this right, the CCPA prohibits a business from selling or sharing the PI of a consumer who is less than 16 years of age absent affirmative authorization from either the minor (in the case of minors who are at least 13 years of age and less than 16) or the parent or guardian (in the case of minors who are under 13 years of age). That prohibition, however, applies only "***if*** the business has actual knowledge that the consumer is less than 16 years of age […]." At the same time, to discourage willful ignorance, the CCPA sets forth that "a[ny] business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age." (*See* Civ. Code Sec. 1798.120(c), emphasis added.). This bill not only requires opt-in consent for the selling and sharing of PI, but also now seeks to require opt-in consent for the collection of PI (Civ. Code Sec. 1798.100) and for the use and disclosure of a minor's PI – and not just sensitive PI (*see* Civ. Code Sec. 1798.121, currently limiting the right to use and disclose sensitive PI).

Mandating across-the-board consent for any processing of minor data, as proposed by **AB 1949**, would impose some of the most stringent privacy restrictions in any jurisdiction and ignores the realities of how consumers engage with businesses. Indeed, under the construct created by **AB 1949**, California's law would be out of sync with all other data privacy laws, creating even greater implementation problems. For example, for companies that operate internationally, the European Union's General Data Protection Regulation permits alternative bases of processing such as "legitimate interest" and "contractual necessity" (e.g., an online store needs consumer data to fulfill an order) that apply to minor data. For businesses that operate nationally, Florida's Digital Bill of Rights explains that the statute shall not be construed to restrict the controller's ability to "provide a product or service specifically requested by a consumer or the parent or guardian of a child, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer before entering into a contract." And for all online businesses operating in the United States, the federal Children's Online Privacy Protection Act (COPPA) provides for some limited exceptions to allow companies to collect information without parental consent. COPPA, of course, also restricts states from imposing liability for regulated activities that are inconsistent with COPPA's treatment of those activities (*see* 15 U.S.C. Sec. 6502.) Thus, without similar exceptions here, businesses not only face significant implementation issues, but also, a real question arises as to whether these new amendments may violate COPPA's preemption clause.

Fundamentally, consent requirements should not extend to low-risk activities and should be reserved for where policymakers believe the processing could impose an actual risk – such as selling data. It should not require consumers to take additional steps to access and experience benign content. Mandating companies to collect such consent would cause a flurry of consent pop-ups and, perversely, requires companies to collect and store *more* data tied to a known minor to comply. The increased collection of data not only creates increased data privacy risks, but research now shows that more pop-ups are leading to "consent fatigue," thus weakening the effectiveness of these disclosures and decisions.

Despite having significant concerns with **AB 1949,** our organizations offered amendments to the author that would have narrowed the bill to a single provision, changing the opt-out rights of 16- and 17-year-olds from the selling and sharing of their PI to an opt-in right, but adding back in actual knowledge. This would have dramatically enhanced the privacy rights of 16- and 17-year-olds for the types of processing activities involving actual risk and would have removed our opposition. Ultimately, Senate Judiciary Committee amendments re-inserted the actual knowledge standard but because the bill was not otherwise narrowed, and because the author subsequently added in additional language undermining the actual knowledge standard yet again (as discussed below), we remain strongly opposed to **AB 1949**.

Actual knowledge standard in the bill no longer seems to require actual knowledge

As noted above, while the need to obtain affirmative authorization is contingent upon the business having "actual knowledge" that the consumer is less than 18 years of age, one of the final amendments to the bill effectively turns that standards upside down, rending it nearly meaningless, if not meaningless. As amended, Proposed Section 1798.139 states that "a business shall treat a consumer as under 18 years of age if the consumer, through a platform, technology, or mechanism, transmits a signal indicating that the consumer is less than 18 years of age." Due to the lack of any other guardrails, let alone definitions, the bill has effectively crafted a blank check to the Privacy Agency to make the law whatever it wishes it to be.

Would an email to an obscure address for the business suffice? Even if it is not intended to handle consumer inquiries and the business has no reason to expect the consumer to transmit a "signal" that they are under 18 years of age? Is the reference to transmitting a signal an indication that the agency can expand what is considered a global opt-out mechanism? What does that look like if AB 3048 (Lowenthal) is signed into law? What if the consumer sends conflicting signals? What if they send a signal that they are under 18 but the business has *actual knowledge* (the consumer also presents them with an I.D. for example to purchase alcohol) that the consumer is 45 years old? Will they violate the law for treating the 45-year-old like any other adult that they have actual knowledge of being an adult? Can they sell alcohol to an individual who states and/or presents as being 45 (verified by ID) but who also sends a separate "signal" that they are under 18? Once again, businesses are compelled to verify each and every consumer's age—which is antithetical to the CCPA's strong privacy protections—and even then, it may not be enough to protect them from liability under **AB 1949**'s newfound understanding of "actual knowledge".

Existing law strikes a careful balance, appropriately mandating opt-in consent for the most vulnerable consumers, for the type of processing that creates the greatest privacy risk.

California's landmark data privacy law, the CCPA, is the result of deliberate policy choices and tradeoffs made between competing consumer privacy rights and business interests. Notably for this bill, in passing AB 375 (Chau & Hertzberg, Ch. 55, Stats. 2018) in 2018, the Legislature rejected a competing ballot initiative proposal which would have treated children's PI as a subcategory of the parent's PI, in favor of a legal construct that instead reflects all of the following principles: (1) a child's PI belongs to the child, not their parent; (2) younger minors face greater vulnerabilities and have significant cognitive differences when compared to 16- and 17-year-olds, warranting greater protections, consistent with other federal and state online privacy laws (*e.g.* Children's Online Privacy Protection Act; Privacy Rights for California Minors in the Digital World); (3) at various ages, minors develop the capacity to exercise various rights independent of their parents as demonstrated, for example, in medical privacy laws[1]; and (4) the greatest risk posed to consumer data privacy rights arises from disclosures made from one entity (with which the consumer interacts), to another.

As a result of such policy choices implicitly embedded into AB 375, the CCPA was crafted to require businesses to receive authorization from a parent or guardian prior to selling the PI of a child under the age of 13, while affording younger teens (13-, 14- and 15-year-olds) the ability to exercise their own opt-in rights, and granting older teens approaching the age of majority (16- and 17-year-olds) the same rights as 18-year-olds. This has the effect of protecting the most vulnerable children (under the age of 16) against the type of processing that posed the most risk (selling data to, or sharing data with, other entities), while effectively creating a ladder for minors that allowed them to gradually understand and assert their rights before turning the age of majority and while still under the supervision of their parent or guardian.

AB 1949 upsets the careful balance struck between competing interests by existing law and runs afoul of data minimization principles

AB 1949 upsets that balance by now treating older teens the same as younger ones, and by expanding the requirements to obtain affirmative authorization (i.e., consent) for any sale or sharing of minors' PI, as well as any collection, use, or disclosure of the minors' PI. This imbalance is exacerbated by removing the actual knowledge standard (*see* comment below) and requiring a business to obtain consent prior to collecting, using, or disclosing the PI *of* a consumer who is under 18-years of age, and not just the PI collected *from* the consumer. Meaning, for example, that any time a parent names their child as a beneficiary or provides the child's PI to receive any benefits, the business will need the consent of their child if the child is at least 13 but under 18 years of age for even the act of collecting the child's name. By way of another example, consider any time a grandparent signs up their grandchild under 18 as their life insurance beneficiary, or an insurance company receives the name of a 16- or 17-year-old employee or driver as part of a worker's comp claim or accident claim. The insurance company will have to obtain the consent of the 16- or 17-year-old before they so much as accept the claim to avoid violating the law. Such a standard is wildly impractical, if not nearly impossible, to implement.

Moreover, insofar as it references the development of an "opt-out signal" to communicate age, **AB 1949** actually runs afoul of the data minimization requirements approved by voters, which clearly states that a business' collection, use, retention, and sharing of a consumer's PI must be "reasonably necessary and proportionate to achieve the purposes for which the [PI] was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes." (*See* Civ. Code Sec. 1798.100(c).)

---

[1] *See e.g.*, Fam Code Sec. 6925, permitting minors to consent to medical care related to the prevention or treatment of pregnancy and to receive birth control without parental consent, and Fam. Code Sec. 6926, allowing minors to consent to confidential medical care services for the prevention of STDs without parental consent, and Health & Saf. Code Secs. 123110(a), 123115(a)(1) and Civ. Code Secs. 56.10, 56.11, preventing the health care provider from informing a parent or legal guardian without the minor's consent and permitting the sharing of the minor's medical information with them only with a signed authorization from the minor).

Requiring affirmative authorization prior to the collection, use, or disclosure of a minor's PI in scenarios where the business does not have actual knowledge will have far reaching impacts for *all* businesses, including brick and mortar stores.

Effectively, **AB 1949** would create strict liability any time the business is wrong, even if the business took every reasonable effort to verify the consumer's age. As such, the bill forces every business covered by the CCPA to collect and validate detailed PI about *every* consumer entering their physical stores or establishments, or websites – in other words, effectively mandating age verification. Of course, accurately confirming a specific individual's age requires gathering more granular information on the consumer, which runs counter to data minimization principles. It is also incredibly impractical.[2]

Consider a brick-and-mortar store that uses video surveillance for security purposes. Given the CCPA's broad definition of PI[3], under **AB 1949**, they would now have to stop every person who looks under the age of 18 to acquire affirmative authorization to capture their image, or their child's image if the minor in question is under the age of 13. If the minor is under 13 and visiting with a friend or family member, they could not be allowed in until the store could contact and receive affirmative authorization from the parent/guardian for that minor. Even running the debit card of a minor as a payment for the good or services that they are purchasing or signing them up for a loyalty program per their request, would require affirmative consent of the minor or their parent/guardian. For that matter, if a 12-year-old so much as submits an order through a mobile app for a beverage at a coffee shop using a gift card they received for their birthday, the store will have to ensure that the parent consents to the collection of the child's name for purposes of completing the order. Conversely if the parent submits an order for food delivery in their 16-year-old's name, the business will need to somehow determine if the named individual is under 18 and obtain consent from that 16-year-old prior to accepting the order. As soon as the order goes through the app to the restaurant, however, the business is assumed to "know" that corresponding name is for a child and not the account holder and will already be in violation of this bill.

Or consider when a minor's family members upload photos of the minor to their private social media account. Platforms will have to take down such photos unless they are able to obtain the consent of any minors in the photo, or their or guardian if the minor is under thirteen. Online services' efforts to implement best practices to detect security incidents, which require collecting and maintaining system logs and other relevant data to monitor suspicious activity such as log-in attempts from new locations or unknown devices, would also be significantly hampered.

Short-term, transient use exemption does not go nearly far enough to address concerns

While amendments sought to clarify that the restrictions placed by **AB 1949** on the use or disclosure of a minor's PI absent affirmative authorization do not prohibit "short-term, transient use of [PI] that is necessary and proportional to the purpose for which it is used" as long as the data is not used, disclosed or retained for any other purpose including building a profile regarding the consumer, they failed to address our concerns – many of which are implicated based on restrictions placed on the *collection* or *disclosure*, and not just the use, of minors' PI. Moreover, as drafted, the amendment may not even operate as intended.

First, by exempting short-term *use* that is necessary "to the purpose for which [the data] is *used*" (as opposed to *collected*), the recent amendments are circular at best.[4] Second, the amendments ignore that there will be instances where completing the transaction or providing service that the consumer has requested requires not only that the business be able to *use* the data for the purpose for which the data is collected, but that the business be able to *disclose* that data to its service provider (e.g. when processing

[2] And in the case of **AB 1949**, it may still be insufficient, if actual knowledge and the consumer's transmitted signal do not align.

[3] "Personal information" generally includes any information that "identifies, relates to, describes, is reasonable capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household[…]." (Civ. Code Sec. 1798.140.)

[4] Compare to: 1798.100(c), which states that "[a] business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes."

payments). Third, even if the amendment is corrected to allow the short-term use *and disclosure* for the purpose for which the data is *collected*, the exemption still ignores the reality that a business would have to lawfully *collect* the PI before it can use or disclose the PI for the purpose for which the data is collected (the amendments do not apply to the restrictions that the bill places around data collection (Proposed Section 1798.100(g)).

AB 1949 will unconstitutionally restrict teens' and adults' access of lawful speech.

Not only is **AB 1949** out of step with the balance struck by the Legislature and voters, as well as with the data privacy statutes of other jurisdictions, but it is also inconsistent with constitutional rights. Again, **AB 1949** requires businesses to obtain "consent" for the collection, use, and sharing the PI of anyone under 18 (and with parental permission for users under 13), with very little exception. Given the CCPA's extremely broad definition of the term, PI is almost necessarily collected anytime someone uses an online service (and many offline services). This provision would violate the First Amendment by effectively requiring businesses to screen a users' age and come up with varying consent options just to access an online service or allow for users to communicate freely online.

Children have First Amendment rights both to receive information and to express themselves. While protecting children from harm is an important interest, **AB 1949** does not attempt to reasonably scope its requirements to that goal, let alone to "narrowly tailor" the law as the Constitution requires. (*Entertainment Software Ass'n v. Blagojevich*, 469 F.3d 641, 646-47 (7th Cir. 2006).) Overall, this policy is not narrowly tailored and would create significant age verification and consent requirements without clearly making services safer or providing more privacy for teens. Given recent lawsuits over similar laws, it is almost certain that constitutional challenges would be raised against **AB 1949** as well.

Mandating parental consent for the collection or use of information assumes all children live in safe, stable, and supportive household environments.

By requiring businesses to seek the consent of a minor's parent or guardian if the minor is under the age of 13, to collect or use any of the minor's PI, this bill will prove problematic if not dangerous to some children who are seeking out information or services that their parent would not approve of. Imagine a 12-year-old wanting to browse books or find resources online to help them grapple with questions around their identity or to obtain necessary mental health services in a household where doing so would put them at risk. The business is placed in the position of having to either obtain parental consent or deny them the important resources that they are seeking out.

Thus, while we agree that the privacy rights of minors are of utmost importance under the CCPA, for the aforementioned reasons, we believe this bill would in fact undermine privacy rights of *all* consumers and we urge you to **VETO AB 1949** (**Wicks**).

Sincerely,

Ronak Daylami
Policy Advocate
on behalf of

American Property Casualty Insurance Association
California Chamber of Commerce
California Retailers Association
Civil Justice Association of California
Computer & Communications Industry Association
Insights Association
Software & Information Industry Association
TechNet