July 8, 2025

TO: Members, Senate Judiciary Committee

SUBJECT: AB 322 (WARD) PRECISE GEOLOCATION INFORMATION
OPPOSE UNLESS AMENDED – AS AMENDED JUNE 23, 2025
SCHEDULED FOR HEARING – JULY 15, 2025

The California Chamber of Commerce and the undersigned must respectfully **OPPOSE UNLESS AMENDED AB 322 (Ward)** as amended June 23 2025, which seeks to amend the California Consumer Privacy Act (CCPA) to expand upon existing protections for precise geolocation information. The CCPA is a comprehensive, industry neutral, and technology neutral statutory scheme that already provides strong consumer privacy protections around the collection, use, and disclosure of all Californians' personal information (PI) – including "geolocation data" as PI, and "precise geolocation"[1] as a form of "sensitive PI" (or "SPI").

We appreciate the approach taken in **AB 322** in comparison to AB 1355 from earlier this year, which appeared to operate as though protections do not exist here in California for SPI and precise geolocation data and would have created far more compliance issues and concerns for CCPA-covered businesses and consumers alike. That being said, while **AB 322's** goal is understandable, its approach could create overly burdensome if not infeasible requirements that do not ultimately serve the purpose of preventing the misuse of precise geolocation data. Unlike most states, California already affords consumers extensive protections over their precise geolocation as a form of sensitive PI under the CCPA as outlined in detail below.

Most pertinent to this bill, businesses not only must: (1) inform consumers exactly how they collect and use this data and (2) disclose for how long they retain it, provided that they do not retain the information for any longer than is reasonably necessary for each disclosed purpose they retain it, but businesses must also (3) provide consumers significant power over how their precise geolocation data is collected and used, giving consumers both: (a) the right to not have additional categories of their SPI collected or used by a business for additional purposes that are incompatible with the disclosed purpose for which their SPI was collected absent consumer notice; and, (b) a right to limit the use and disclosure of their precise geolocation purposes to only a narrow set of permissible purpose that includes providing the goods or services requested by a consumer or detecting abuse and illegal activity, for example.

While we do not question the bill is well-intentioned and understand it may be tempting to explicitly restate elements of these existing rights in a new bill as they apply to precise geolocation given current events, doing so suggests that existing laws are somehow deficient or inapplicable. This risks creating confusion about the scope of current law and, paradoxically, may weaken those protections.[2] We also note that this

[1] Defined under Civil Code Sec. 1798.140(w) as "any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, except as prescribed by regulations."

[2] As Civil Code Section 3532 provides, "[t]he law neither does nor requires idle acts." Courts interpret statutes to avoid requiring pointless or redundant actions or outcomes that serve no new legal or practical purpose. In other words, laws must effectuate change and provide meaningful direction, not merely restate what is already true. In that light, arguably, the safer and more constructive approach here would be to enact a resolution recognizing and reaffirming the rights that already exist at law in California.

is not the first time the Legislature has grappled with concerns over how to best protect information against being handed over in an unchecked manner to certain entities like law enforcement or other states with conflicting views on civil liberties to California, post-enactment of the CCPA.[3]

If the desire is to strengthen existing law, there are more tailored ways to do so that would be less duplicative and cause less confusion than **AB 322**. But as outlined in this letter, California has gone to great lengths to ensure that sharing of PI to certain entities is *not* unchecked and without significant limits. As drafted, however, **AB 322** remains vastly problematic in its unnecessarily duplicative and overlybroad approach in some aspects and infeasible requirements in others. As such, we ask that you consider more targeted ways of addressing these issues and stand ready to have those conversations about how as the bill moves forward. Given the volume of bills and the recent nature of these amendments we have done our best to start to outline some of our suggestions in this letter but look forward to providing more tailored redlines to address our concerns fully, shortly.

An overview of how exactly existing law ensures that consumers can limit the use and disclosure of their sensitive PI, including precise geolocation data

As you know, consumers already have significant protections around how their location data can be collected and used by businesses under the CCPA, and by government entities under the California Electronic Privacy Act (CalECPA).

That is partly why earlier this year our organizations vehemently opposed AB 1355 (Ward, 2025)[4] on geolocation data – not merely because it expanded on those rights, but especially because it would have placed new restrictions around location data collection and use practices by businesses in California in a manner that will undermine and cause confusion with the California Consumer Privacy Act, which already addresses these policy questions and data privacy concerns and has done so since the law was first enacted in 2018. Those initial protections which were added in the original CCPA legislation, AB 375 (Chau and Hertzberg, Ch. 55, Statutes of 2018) and reaffirmed and further strengthened by voters with the inclusion of new rights and controls over "sensitive PI" including the new category of "precise geolocation" information via Proposition 24 in 2020. While the rights have been in place statutorily for several years now and many consumer advocacy groups will state that it is clear those rights are in adequate, in actuality, regulatory changes were also necessary to effectuate CCPA changes both after the enactment of the original law and after the enactment of Proposition 24. It was only on March 31, 2023, that the new California Privacy Rights Agency even finished finalizing the regulatory framework that implemented the expansion of the new rights such as the rights for sensitive PI and precise geolocation.[5]

Under the CCPA, which is enforceable by way of administrative and civil actions brought forth by the California Privacy Protection Agency and the Attorney General[6], a consumer has the following rights which

[3] AB 523 (Irwin, 2019) presented the first conversation around whether there needed to be separate rules in certain circumstances. The Assembly Privacy and Consumer Protection Committee did not pass that legislation at that time either, over similar concerns related to the confusion that would be caused when the CCPA already covering precise geolocation information, noting also that an opt-in approach within the CCPA would have avoided confusion if that were the intent. Unfortunately, that would have caused some confusion with federal opt-out requirements, which is why many in the business community understandably still opposed that legislation as well.

[4] That bill was ultimately held in the Assembly Appropriations Committee on the Suspense File.

[5] We note this to say that the CCPA is not an uncomplicated law to implement. It is vague, onerous, and therefore costly in many aspects. Using the State's own figures, the Privacy Agency's most recent Standardized Regulatory Impact Assessment (SRIA) for their current rulemaking concludes that the regulations would result in direct costs to California businesses of $3.5 billion in the first full year and average annual costs to businesses over the first ten years of $1.08 billion. Even still, CalChamber commissioned well-respected economists to conduct an analysis of the Agency's SRIA, including by former Director of Finance, Michael Genest, and that report found that SRIA's estimates were wildly inaccurate to the tune of several billions of dollars in costs in the first year and dramatically overstated the long-term benefits. This is not an uncomplicated law that could be enacted overnight.

[6] Only the AG may bring both administrative and civil actions, the CPPA may only bring administrative.

are most pertinent to this bill, when it comes to the collection, use, and disclosure (including the selling/sharing) of their PI and SPI[7], among other things:

1. **The right to be told at or before the point of collection**, certain information, including **the categories of PI and SPI to be collected about consumers** and the purposes for which they are to be used and whether that information is to be sold or shared. (Civ. Code Section 1798.100(a).)
2. The **right to not have additional categories of their SPI collected or used by a business for additional purposes that are incompatible with the disclosed purpose for which their SPI was collected absent consumer notice**. (.100(a).)
3. **The right to know how long a business intends to retain each category of their data**, **provided that their data shall not be retained for each disclosed purpose longer than is reasonably necessary for that disclosed purpose**. (.100(a).)
    - Third parties controlling the collection of PI about a consumer may satisfy their obligations by providing the required information prominently and conspicuously on the homepage of their internet websites. (.100(b).)
    - A business that collects a consumer's PI and that sells that PI to a third party or that discloses it to a service provider or contractor for a business purpose must enter into an agreement with that third party, service provider, or contractor, that among other things: (1) specifies that the personal information is sold or disclosed by the business only for limited and specified purposes and (2) *obligates the third party, service provider, or contractor to comply with applicable obligations under the CCPA and provide the same level of privacy protection as is required under the CCPA*. (.100(d).)
4. **The right to limit the use and disclosure of SPI** to **that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services** (.121)**, and to perform specified, limited "business purposes" under the CCPA,** such as helping to ensure security and integrity to the extent the use of the consumers PI is reasonably necessary and proportionate for these purposes, or as authorized by regulations [*see* also .140(e)(2)(4)(5) and (8)].
    - Notably, a business that has received such a direction from a consumer is prohibited from doing so for any other purpose after receipt of that request, except as specified above, unless the consumer subsequently provides consent for additional purposes.
    - Additionally, any service provider or contractor that assists a business in performing one of these authorized purposes may not use any sensitive PI it received about that consumer pursuant to a written contract with the business either, after it has received instructions from the business to limit the use and disclosure of the consumer's SPI, and to the extent it has actual knowledge that the PI is sensitive PI for any other purpose.
5. **The right to request deletion of their own PI that was collected *from* them** (.105); **to know what PI is collected about them and access their own PI** (.110); **to know what PI is "sold" (i.e. disclosed) and to whom** (.115); **and the right to opt out of the sale if the consumer is age 16 and over and alternatively the right to opt-in if the consumer is under 16 years of age** (.120).

---

[7] Notably, under this CCPA, these terms were intentionally defined incredibly broadly such that information is considered "PI" even if it does not actually identify or describe a particular person or household but is at least reasonably capable of being associated with or could be reasonably linked, directly or indirectly, with a particular person or household.

"Collection" means obtaining the information in any sort of way—actively or passively. And "selling" does not require that you have sold it to another person for monetary exchange, any sort of disclosure for valuable consideration (such as customer list exchanges) will suffice.

Virtually everything is covered, unless it is aggregated data, publicly available information, or deidentified information, or it is subject to a specific exemption. PI expressly includes geolocation data, and it also includes identifiers such as online identifiers, IP addresses, other similar identifiers, as well as biometric information and audio, electronic, visual, or similar information. (Civil Code Sec. 1798.140(v).)

- This includes the right to be notified by third parties to whom their data is sold/shared, and given an explicit opportunity to opt out before their data is further sold or shared. (.115(d).)

Moreover, the CCPA clearly outlines the ways in which a business must comply with these rights via both detailed notice, disclosure, correction, and deletion requirements in Section 1798.130 and detailed requirements outlining the methods to be provided to limit the sale, sharing, and use of PI and the use of sensitive PI in Section 1798.135.

Many of these provisions render the requirements of this bill redundant and unnecessary as they would cause confusion or otherwise suggest that existing law does not have these exact same effects. For example, Section 1798.100, .110, .115, and Section 1798.130 together render Proposed Section 1798.122(a) duplicative and unnecessary because the CCPA already requires similarly specific disclosures to consumers about the collection, processing or sharing of any of their sensitive PI, including precise geolocation data, as outlined above. At minimum, significant narrowing amendments would be necessary to avoid duplication, better align with the CCPA's existing requirements, and to avoid the implications that apps have to present notices in devices' settings menus and/or constantly display massive notices to consumers for long periods during which they are using an app—issues outlined in the section below.

- ***To that end, we suggest striking subdivision (a) from the bill.*** *Doing so would address the concerns outlined in the section below as well.*

- *Also, as a drafting matter, we suggest changing references from "precise geolocation information" to "precise geolocation" to stay consistent with the terminology used in the CCPA.*

Practical compliance challenges of AB 322's notice requirements

As noted above, existing law already requires that consumers receive notice about what PI and SPI is collected at or before the point of collection and what categories of PI is collected from them[8] in Sections 1798.100 and 1798.110 and delineates how that notice and disclosure is to be provided to consumers in Section 1798.130 rendering Proposed Section 1798.122(a) redundant and confusing. That section has other ailments however, including that it is drafted in a manner that would be virtually impossible, if not impossible, for businesses to comply with. These largely stem from the "real time" disclosure requirements. Under **AB 322**, notices for virtually the same information that is already provided under the CCPA would now have to be provided "*when precise geolocation information is being collected* … to the consumer whose precise geolocation information is being collected." (*See* Proposed Section 1798.122(a).)

It would be incredibly (and unreasonably) difficult if not impossible to constantly signal to a consumer that location data is being collected when that is necessary for the services. When a business seeks to collect precise geolocation information from a consumer's device via an app, for example, the app itself is not the entity directly obtaining the consumer's permission. From both a technical and privacy standpoint, apps receive a device's precise geolocation information only if device users enable the sharing of that information with specific apps in the devices' settings menu. In other words, although apps can provide users with information in their apps about how precise geolocation information will be used, the actual act of collecting the information for the first time – and the presentation of notices to consumers when the permission is actually sought – happens in devices' settings menus, not in apps.

As such, subdivision (a) could be read to mean that apps would be required to somehow present notices to consumers in devices' settings menus - something apps have no control over. It could also be read to mean that a notice would have to be presented to consumers for the entire duration of time during which their precise geolocation is being collected. This would not be possible to do without significantly degrading

[8] While Sections 1798.110 and .115 only mention "categories of [PI]", Section 1798.130 clearly states that "(c) [t]he categories of [PI] required to be disclosed pursuant to Sections 1798.100, 1798.110, and 1798.115 shall follow the definitions of [PI] and sensitive [PI] in Section 1798.140 by describing the categories of personal information using the specific terms set forth in subparagraphs (A) to (K), inclusive, of paragraph (1) of subdivision (v) of Section 1798.140 and by describing the categories of sensitive [PI] using the specific terms set forth in paragraphs (1) to (9), inclusive, of subdivision (ae) of Section 1798.140."

consumers' experiences. It would require, for example, that a user trying to navigate within an app would have a large portion of their screen constantly taken up with a notice listing all of the types of information specific in section (a) - something no consumer wants.

Putting aside that the CCPA already includes significant notice requirements and regulatory standards for how to communicate notices to consumers which render this unnecessarily onerous at best, *it is also important to consider that devices like iPhones already provide visual cues to consumers whenever their location is being used. On iPhones, this appears as an arrow that's persistently present at the top of the screen.*

Furthermore, **AB 322**'s notice requirement requires that the consumer notice now state a telephone number and internet website through which the consumer can obtain more information. This is both duplicative in some cases, but not possible from a compliance standpoint in other cases, causing unnecessary confusion. Section 1798.130 of the CCPA already requires that consumers be given, in a form that is reasonably accessible to them, two or more designated methods for submitting requests to find out what categories of PI and SPI has been collected or sold about them, including at minimum a toll-free telephone number (unless a business operates exclusively online in which case they only have to provide an email address) plus an internet website if they maintain one. A business that does not have to provide a telephone number under the CCPA is now being told under **AB 322** that they do and would be put in a position to violate **AB 322** [via Proposed Section 1798.122(a)] if they were to rely on the CCPA [via Section 1798.130 (a)(1)].

Retention limitations are unreasonable and arbitrary, impeding businesses' ability to conduct basic activities

With regard to Proposed Section 1798.122(b)(1)(A), we believe amendments are needed to **AB 322** both to recognize the substantial protections already exist under California law for precise geolocation data and to align this bill to those protections, which include including data minimization rights and data retention limitations.

As noted above, California law already requires that consumers be told, at or before the point of collection the length of time that a business intends to retain each category of SPI or if that is not possible, the criteria used to determine that period. The law also requires, however, that precise geolocation data, like all sensitive PI – and all PI for that matter – be collected or processed for no longer than is reasonably necessary and proportionate to achieve the purposes disclosed to the consumer. (*See* Civ. Code Sec. 1798.100.) And, as also mentioned above, if a business processes precise geolocation data beyond a set of permissible purposes, California law already creates a consumer right to limit those uses to only those limited permissible purposes, consistent with data minimization principles. (*See* Civ. Code Sec. 1798.121.)

In contrast, **AB 322**'s retention requirements under Proposed Section 1798.122(b)(1)(B)(ii) and (b)(2), would impose arbitrary limits that would impede businesses' ability to conduct basic activities, and put them in legal jeopardy.

Specifically, **AB 322** prohibits a business that collects and processes precise geolocation information from collecting or processing "more than necessary to provide the goods or services requested by the consumer" [via (b)(1)(A)] unless it is to respond to security incidents, fraud, harassment, malicious or deceptive activities, or any illegal activity targeted at, or involving, the controller or processor or its services or to investigate, report, or prosecute those responsible for any of those actions [(b)(1)(B)(i)] and limits retention of that information for these specifically enumerated purposes to no more than 30 days [(b)(1)(B)(ii)].

Separately, **AB 322** prohibits a business that collects precise geolocation data from retaining precise geolocation data longer than is necessary to provide the goods or services requested by the consumer or longer than one year after the consumer's last intentional interaction with the business, whichever is earlier. [via (b)(2).] For example:

- The longer retention periods provided in subdivision (b)(2) do not specifically apply to the fraud and security language uses as the fraud and security exception applies only to the limitation placed on collecting and processing precise geolocation. As such, the bill fails to recognize that when precise

geolocation information is used to investigate and respond to security incidents and other threats and illegal activity, retention beyond 30 days is often necessary. This is important as it often takes more than 30 days for a company to be able to fully investigate and reach a determination about whether someone's account may have been hacked or is being used for fraud.

- These sections fail to recognize that precise geolocation information often has to be retained longer than "30 days," or even longer than is "*necessary* to provide the goods or services requested by the consumer" or even "longer than one year after the consumer's last intentional interaction" in order to conduct future troubleshooting, identify and repair technical issues, improve products and services, and more. Consider for example if the information is needed for an extended warranty. Ensuring that businesses can retain precise geolocation information for the purposes they disclose to consumers would solve this problem.

  Moreover, what is necessary is highly debatable and subjective. For example, would it be necessary to provide regionally relevant ads to those located at or near a sports arena? This exposes businesses to great uncertainty as to whether they are permitted to retain information.

"Re-sale" limitations to third parties

We recognize that prohibiting the sale of precise geolocation data to unrelated third parties as suggested in Proposed Section 1798.122(b)(3) is potentially a more tailored approach similar to what we argue for below, and consistent with the spirit of the existing CCPA. At a minimum, however, we believe it is important to ensure that the prohibition and terminology used in that prohibition be amended to better align with the CCPA to avoid regulatory confusion given the fact that the CCPA has a broader definition of sale than any other state privacy law. That being said, an outright prohibition can have long lasting implications that we cannot yet fully understand the implications thereof. While we are considering other solutions to offer here, at minimum amendments are needed to:

- ***strike new terms like "lease' and "trade"—noting, of course, that the term "sale" under the CCPA is incredibly broad, rendering the use of these terms is unnecessary in the first place***.

State and local agencies are subject to CalECPA restriction in accessing location data and several California bills have previously been specifically passed to protect the civil liberties of Californians

We think it is also important to note that all governmental entities are subject to the California Electronic Privacy Act (CalECPA) enacted by way of AB 178 (Leno, Ch. Stats. 2015) in response to concerns that the law had not been adequately updated to protect all forms of electronic communication and metadata. As acknowledged in prior Assembly Privacy and Consumer Protection Committee analyses, AB 178 "required a demonstration of probable cause to obtain electronic communications information from a third-party service provider, responding to a high percentage of legally inadequate requests from law enforcement. It also applied the probable cause requirement to past electronic communications, regardless of their age, which was an improvement over federal law. SB 178 also guaranteed that geolocation information is protected by the same standard, which codifies protections established in case law […]. The author's end goal with SB 178, according to the Assembly Floor analysis, was to create a 'clear, uniform warrant rule for California law enforcement access to electronic information.'" [*See* AB 1638 analysis (2019-2020 Regular Session), pp. 3-4.] Again, we caution against undermining existing protections that exist at law and suggesting or misleading entities into believing that information can be handed without proper legal paperwork demanding production or exigent circumstances consistent with the Fourth Amendment.

We are of course ready to work with you and this Legislature on a proposal that makes sense for the concerns identified, and simply caution that in the absence of **AB 322**, there are significant safeguards in place both under the CCPA and CalECPA, as well as other statutes enacted over the years, such as AB

1242 (Bauer Kahan, Ch. 627, Stats. 2022[9]); AB 1747 (Ch. 789, Stats. 2019[10]); SB 54 (De León, Ch. 495, Stats. 2017[11]); AB 450 (Chiu, Ch. 492, Stats. 2017[12]); AB 2792 (Bonta, Ch. 769, Stats. 2016[13]), to name a few.

Disclosure to out-of-state jurisdictions and federal law enforcement

Proposed Section 1798.122(b)(4) appears aimed at guarding against the potential disclosure of precise geolocation information to a state or local law enforcement entity from out of state that is attempting to investigate or prosecute individuals for reproductive healthcare-related activity that would be legal in California. As noted above, California has gone to great lengths to add such protections under existing law, both by way of AB 1194 (Carrillo, Ch. 567, Stats. 2023)[14], and AB 1242 (Bauer-Kahan, Ch. 627, Stats. 2022). The latter enacted California's shield law specifically to provide robust protections against this risk.

That law prohibits companies that provide electronic communication services or remote computing services from complying with out-of-state warrants *unless they are accompanied by attestations that the evidence sought is not related to an investigation into, or enforcement of, violations of laws creating liability for providing, facilitating, or obtaining an abortion that is legal in California*. Importantly, this covers warrants seeking, among other things, "data stored by, or on behalf of" consumers, as well as records revealing consumers' "usage of" the companies' services; these categories could include exactly the kind of precise geolocation information **AB 322** is trying to protect.

Not only does **AB 322** fail to recognize the protections of AB 1242 in this subdivision, but it would also put businesses in an impossible position. Assuming a business could determine whether an out-of-state court order "is consistent" with California's laws – something that is arguably better suited for the courts – deciding that an order is not consistent would force the business to violate either **AB 322** or the other state's law. That is precisely why AB 1242 created the attestation process. **AB 322** would now put companies in an impossible compliance position.

- ***As such, we suggest either removing paragraph (4) entirely, or narrowing it substantially to better align with AB 1242.***

Moreover, Section 1798.122(b)(5) is designed to address the potential disclosure of precise geolocation information to federal law enforcement, including ICE.

---

[9] Prohibiting California corporations or corporations whose principal executive offices are located in California from producing pursuant to a warrant, court order, or subpoena, any records, electronic communications, or other information that the corporation knows, or should know, relates to an investigation or enforcement of a "prohibited violation" (i.e., a violation of a law that creates liability for, or arising out of, either providing, facilitating, or obtaining an abortion or intending or attempting to provide, facilitate, or obtain an abortion that is lawful under California law.). Also prohibiting law enforcement agency from cooperating with, or giving information to, a person, agency, or department from another state regarding a lawful abortion performed California and protected under California laws.

[10] Prohibiting subscribers of the California law Enforcement Telecommunications System (CLETS) from accessing non-criminal history information transmitted through the system for immigration enforcement purposes.

[11] Enacting the California Values Act, limiting local and state law enforcement agencies from using resources for immigration enforcement purposes and restricting sharing personal information with federal immigration authorities without judicial warrant.

[12] Generally requiring employers to notify employees of any ICE audit or inspect of employment records.

[13] Enacting the TRUTH Act, enhancing transparency in local law enforcement communication with ICE and requiring law enforcement agencies to provide individuals with written consent forms explaining their rights before an interview with ICE.

[14] This bill amended the CCPA to limit exemptions that allowed permitting businesses from disclosing data to law enforcement if the data related to PI that contains information related to accessing, procuring, or searching for services regarding contraception, pregnancy care, and perinatal care, including, but not limited to, abortion services. AB 1194 also demonstrates that such a broad policy shift is clearly not necessary to provide additional protections for Californians to keep data from being transferred to certain entities.

- ***We believe only minor, clarifying amendments are needed to paragraph (5), that companies may be permitted—if not required—under federal law to disclose information in a narrow set of circumstances, such as to seek investigation into crimes committed on businesses, or to comply with court orders or fourth amendment demands under exigent circumstances.***

Again, we greatly appreciate and thank you for the better direction of this bill, compared to AB 1355 but have significant concerns over the redundancy and the overly broad approach taken in this bill and the confusion it will cause, not to mention how it may undermine existing protections. While we do plan to provide a redline of suggested amendments shortly that take into consideration the concerns and suggestions above, we must **OPPOSE UNLESS AMENDED AB 322 (Ward).**

Sincerely,

Ronak Daylami
Policy Advocate
on behalf of

California Chamber of Commerce, Ronak Daylami
California Retailers Association, Ryan Allain
Computer & Communications Industry Association (CCIA), Aodhan Downey
Security Industry Association, Jake Parker
Software Information Industry Association, Anton Seventer
TechCA, Courtney Jensen
TechNet, Robert Boykin

cc: Legislative Affairs, Office of the Governor
Charles Loudon, Office of Assemblymember Ward
Consultant, Senate Judiciary Committee
Morgan Branch, Consultant, Senate Republican Caucus