March 25, 2025

TO: Members, Assembly Privacy and Consumer Protection Committee

SUBJECT: AB 1355 (WARD) LOCATION PRIVACY
OPPOSE– AS INTRODUCED FEBRUARY 21, 2025
SCHEDULED FOR HEARING – APRIL 1, 2025

The California Chamber of Commerce and the undersigned must respectfully **OPPOSE AB 1355 (Ward)** because it seeks to place 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. 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 – including location data.

That has been the case since the law was first enacted in 2018, and voters both reaffirmed that in 2020 and strengthened those protection when they made a consumer's precise geolocation sensitive personal information as well, granting the consumer additional privacy rights and controls over that information. Notably, it was only on March 31, 2024, that the new California Privacy Rights Agency even finished finalizing the regulation that implemented the expansion of new rights under that proposition, yet at every turn businesses face more legislation that seeks to duplicate rights and renegotiate elements of the law in new statutes outside of the CCPA.

Now, despite California's existing protections for location data and precise geolocation data, **AB 1355** would:

(1) prohibit a "covered entity" from collecting or using the location information of an individual unless doing so is necessary to provide goods or services requested by that individual and the individual has opted into the collected or use of their location information for that purpose;

(2) impose various other restrictions for location information, defining it as information that pertains to or reveals, whether directly or indirectly, the present or past geographical location of an individual or device—regardless of whether the location was from recent history and might present some reasonable danger to the person or would simply place the individual in a particular continent at one point in their lifetime;

(3) further require covered entities to prominently display a specified notice to individuals, at the point where location information is being collected, stating that their location information is being collected, the name of the covered entity and service provider collecting the information, and a phone number and an internet website where the individual can obtain more information;

(4) require covered entities to maintain and make available to the data subject a location privacy policy that includes specified information on data usage and management and is subject to a specified notice procedure;

(5) make covered entities that violate these provisions liable for actual damages suffered by a person denied a right under these provisions and other specified relief;

(6) authorize the Attorney General or other public prosecutors to bring an action against covered entities that violate these provisions; and,

(7) prohibit any state or local agencies from monetizing location information.

There are several practical consequences of these proposed changes that should be seriously considered as outlined further below.

AB 1355 Unnecessarily Creates Confusion in Operability for Businesses Already Taking on Significant Compliance Costs to Implement the CCPA

AB 1355 creates confusion not only in terms of operability with the CCPA by providing alternate and conflicting restrictions around the use and disclosure of this specific type of personal information. 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) (*see below* for more).

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[1], a consumer has the following rights, relevant to this bill, when it comes to the collection, use, disclosure (selling/sharing) of their personal information (PI).

Notably, under this act, these terms were defined incredibly broadly such that information is considered "PI" even if it doesn't 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[2], 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).)

Of particular importance to **AB 1355**, in 2020, voters approved additional protections under the CCPA for SPI, including precise geolocation data. Under Proposition 24, precise geolocation data was therefore included to expand the existing CCPA protection and also add special protections to (1798.140(ae)) "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." (1798.140(w).) All of these terms, of course, are comparable to, if not even broader than, location information under **AB 1355**.

Substantively, these CCPA rights include, among other things:

- **The right to be told at or before the point of collection**, certain information, including **the categories of personal information (PI) and sensitive PI (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).)

[1] Only the AG may bring both administrative and civil actions, the CPPA may only bring administrative.
[2] And even then, under the CCPA, there is specific meaning ascribed to that term which requires you to keep such information de-identified in order for the exemption to apply –otherwise it becomes PI once again.

- The right for a business to not collect additional categories for SPI or to use SPI collected for additional purposes that are incompatible with the disclosed purpose for which the SPI was collected without consumer notice. (.100(a).)
- The right to not have their data 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 obligation 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).)
- **The right to request deletion of their PI.** (.105)
- **The right to know what PI is collected about them and access their own PI.** (.110)
- **The right 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 age16 and over and alternatively the right to opt-in if the consumer is under 16 years of age** (.120). 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).)
- **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, 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 (.121; .140(e)(2)(4)(5) and (8).)

  Notably, a business that has received direction from a consumer not to use or disclose the consumer's SPI, except as authorized by subdivision (a), shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section 1798.135, from using or disclosing the consumer's sensitive personal information for any other purpose after its receipt of the consumer's direction unless the consumer subsequently provides consent for the use or disclosure of the consumer's sensitive personal information for additional purposes.

As you can see, the elements of **AB 1355** (and more) are well covered under the CCPA but for the difference in opt-in versus opt-out and the banning of monetization by state and locate agencies.

Changing the rules has real economic cost to businesses and consumers; constantly doing so without adequate justification or need is irresponsible at best.

Since these rights were first adopted in June 2018 as an urgency act in AB 375 (Stats. 55, Stats. 2018) and expanded in 2020 by way of Proposition 24, effective January 1, 2023, businesses have been working to come into compliance – which has not been made any easier due to the Privacy Agency's significant delays in issuing implementing regulations. While regulations were ordered to be completed by July 2022, the first part of the regulations were not competed until the very end of March 2024 – less than 1 year ago. The formal rulemaking process for the second part is still ongoing.

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.

Adding additional compliance challenges creates confusion by having parallel regulatory constructs for geolocation data which is not only unnecessary, but arguably incredibly fiscally irresponsible under such circumstances. It is important not to lose sight that the CCPA is not a law governing big tech. It governs brick and mortar stores as much as it does online ones; startups, small businesses, medium sized, and large alike. **AB 1355** does not appear to be different in that regard. Only now, the burdens would be two-fold with location data being covered twice.

There are More Narrow Public Policy Options to Address Concerns as Evidenced by Other Recent Legislation

Not only is this bill unnecessary, but we note that there are other policy approaches that would be more viable approaches to strengthening existing law, should that be the desire. We note that this is not the first time the Legislature has grappled with these concerns post-CCPA.[3]

We note that as recently as 2023, AB 1194 (Carrillo, Ch. 567, Stats. 2023) 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. First, this would also provide additional protections in terms of geolocation data, but also, if there are other similar concerns related to when geolocation data might be requested, AB 1194 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.

Unintended consequences of AB 1355 – both from a business and public safety perspective

Should **AB 1355** move forward, there are a host of practical outcomes that should be considered. To name just a few, but not all:

- **Emergency Alerts.** The sale of precise geolocation data powers important emergency notices, such as missing children alerts and severe weather alerts. The sale or transfer of precise geolocation data allows AMBER alert notices as well as information regarding extreme weather to be immediately displayed to users in the impacted area on any device they are using. Even if you exempt the use of data for certain emergency purposes, if **AB 1355** becomes law, precise geolocation data will lose much of its utility in the marketplace. As a result, this data will be less likely to be collected and used, making it less procurable for use for emergency alert purposes. Californians may therefore lose access to these important, real-time alerts, which rely on the transfer or sale of precise geolocation data.

- **Advertising and Marketing.** The modern digital economy relies on data being available from third parties and on the programmatic exchange of data, which often constitute a "sale" under state law. Precise geolocation data is an integral component for consumer personalization and marketing that allows companies to reach consumers with relevant content and ads at the right time and in the right place.

  For example, an owner of a newly open restaurant with limited marketing budget would like to advertise to individuals within two miles of its location. By working with an advertising company, that local business owner can target devices that have opted into the processing of geolocation data within two miles of the restaurant with a targeted ad. Without the ability to sell or transfer such data subject to consumer consent, businesses will have a more difficult time, and a higher cost, reaching consumers

[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.

with relevant marketing and consumers will not be alerted to products and services they desire that are near to them.

- **Identity and fraud protection.** Financial institutions, retailers, and others rely on anti-fraud services that include precise geolocation data provided by third parties. The sale of precise geolocation data allows anti-fraud and identity protection services to flag suspicious behavior and protect vulnerable communities. For example, companies can more easily detect credit card theft or fraud if they or their service providers have access to precise geolocation data showing that a consumer is not in the location where a purchase is being made. The ability to use and transfer precise geolocation data helps companies to detect and prevent fraudulent and illegal activity and reach out to consumers to confirm their purchases. Again, even if **AB 1355** were to exempt uses of data for anti-fraud purposes, companies may collect and use it less, making it less available for this important anti-fraud and identity protection use. Meaning, the bill would still inhibit the use of precise geolocation data to protect consumers from fraud and identity theft in effect.

- **In some contexts, it not entirely clear what might be "necessary to provide goods or services requested by that individual".** For example, hospitals put location anklets on newborns. An alarm sounds if the baby is taken out of the perinatal area, and there's a tracker so the hospital can find the baby if someone tries to kidnap it. The anklet is removed when the baby is discharged. Assuming that's not "necessary to provide goods or services requested by the individual," if a mother comes in on an emergency basis and prior consent cannot be obtained, what then? Also, hospitals often track their equipment. If they were to have a tracker on an infusion pump and a patient is hooked up to the infusion pump, would this bill consider them to be tracking the patient? Is an opt-in needed?

  Neither of these situations appear covered by the exemption for data collected from a patient by a health care provider or health care facility, or collected, processed, used, or stored exclusively for medical education or research, public health or epidemiological purposes, health care treatment, health insurance, payment, or operations, if the information is protected from disclosure under the federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1), or other applicable federal and state laws and regulations pertaining to health care privacy.

- **Definition of "individual" has broad implications for certain industries and for public entity employees as well.** The broad definition of individual captures both consumers and employees, which especially raises concerns for certain industries involving commercial vehicles where GPS devices are needed to track equipment, but also from a state and federal government mandate for employee drivers to utilize an electronic logging device (e.g. the trucking industry).

  And because "individual" is so broad that it captures both private and public employees, **AB 1355** will also impact any entity, public or private, that maintains location data for its employees, via a tracking system for its vehicle fleet, phone, or other technology, if a private vendor is involved or the data is maintained in a cloud maintained by a private entity[4]. Any location tracking will require employers to receive consent from an employee in order to track a vehicle for an employee's safety, because a job site is in a remote location, or for security, because their vehicles or materials inside are highly valuable.

- **Definition of "location information" does not exclude publicly available data including data that is collected from public records**. There are First Amendment rights to data in such records, which is why the Legislature passed AB 874 (Irwin, Ch. 748, Stats. 2019) following the passage of the CCPA, to ensure that the rights of privacy did not unlawfully infringe upon First Amendment rights. Voters in fact expanded upon the exception passed by the Legislature in AB 874 in Proposition 24, so this would directly contravene voters' intent. Doing so by enacting a new statute on the same issues, as opposed to amending the existing statutes does not change that fact.

- **Preexisting data**. What of all preexisting data? Does the bill apply prospectively only? Or does it apply to all data currently in existence?

[4] This depends in part how broadly "obtain, infer, generate, create, receive, or access an individual's location information" is interpreted for purposes of "collect[ion]" under **AB 1355**.

Penalties under this bill will devastate businesses and are contrary to the intent to have a limited private right of action under the CCPA while businesses still work to implement the law

Under **AB 1355**, any person who "denies a right protected by this title, or aids, incites, or conspires in that denial, is liable for each and every offense for the actual damages suffered by any person denied that right *plus* all of the following:

(1) An [*uncapped*] amount to be determined by a jury, or a court sitting without a jury, for exemplary damages.

(2) A $25,000 statutory civil penalty, to be awarded to the person denied their right under the bill – this is regardless of actual damages being shown.

(3) Preventive relief, including permanent or temporary injunction, restraining order, or other order as specified; and,

(4) Reasonable attorney's fees and costs, including expert witness fees and other litigation expenses, to a prevailing plaintiff only.

Notably, there is no requirement that actual damages be proven in order to get exemplary damages or statutory damages. Meaning, these varying damages may just be tacked on to one another, with exemplary damages of an uncapped amount and statutory damages of a guaranteed $25,000 amount constituting the absolutely floor—per each and every offense. And while there is absolutely no clarity on what constitutes "each and every offense", the phrasing easily creates that plaintiffs' attorneys will construe this to maximize violation and payouts.

Further, with "covered entities" including any individual, partnership, corporation, LLC, association, or other group, however organized, including all the agents of the entity, this will not only bankrupt small businesses, but bankrupt each individual involved (the bill, of course, gives no guidance as to what constitutes aiding, inciting, or conspiring), personally, to ensure they cannot recover any time soon.

It goes without saying that this bill is not only inconsistent with the intent of the Legislature and voters who intended the CCPA to have a limited private right of action while such massive shifts in public policy where enacted in our data privacy practices—including around location data--but it creates significant liability risks for businesses, opening the floodgates on lawsuits that are based on minor, technical violations, instead of actual injury.

State and local agencies are subject to CalECPA restriction in accessing location data

While we cannot speak to how state or local agencies may or may not monetize location information, we do 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.]

Thus, in the absence of AB 1355, 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[5]); AB 1747 (Ch. 789, Stats. 20196); SB 54 (De León, Ch. 495, Stats. 20177); AB 450 (Chiu, Ch. 492, Stats. 20178); AB 2792 (Bonta, Ch. 769, Stats. 20169), to name a few.

Ultimately, if there is going to be a policy discussion around opt-in versus opt-out, it should be had within the context of the CCPA—not outside of it, and it should be done with a full recognition of all the statutory protections that exist in this state. **AB 1355**, in contrast, appears to operate as though these protections do not exist here in California.

But for the aforementioned reasons, we strongly **OPPOSE AB 1355 (Ward).**

Sincerely,

Ronak Daylami
Policy Advocate
on behalf of

Association of California Life and Health Insurance Companies, Chloe Shin
Association of National Advertisers, Christopher Oswald
CalBroadband, Amanda Gualderama
California Chamber of Commerce, Ronak Daylami
California Credit Union League, Eileen Ricker
California Financial Services Association (CFSA), Scott Govenar
California League of Food Producers, Katie Little
California Retailers Association, Ryan Allain
Computer & Communications Industry Association (CCIA), Aodhan Downey
Consumer Data Industry Association (CDIA), Kris Quigley
Insights Association, Howard Fienberg
Security Industry Association, Jake Parker
Software Information Industry Association, Abigail Wilson
TechCA, Courtney Jensen
TechNet, Robert Boykin

cc: Legislative Affairs, Office of the Governor
Consultant, Assembly Privacy and Consumer Protection Committee
Charles Loudon, Office of Assemblymember Ward
Liz Enea, Consultant, Assembly Republican Caucus

RD:ldl

---

[5] 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.
[6] Prohibiting subscribers of the California law Enforcement Telecommunications System (CLETS) from accessing non-criminal history information transmitted through the system for immigration enforcement purposes.
[7] 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.
[8] Generally requiring employers to notify employees of any ICE audit or inspect of employment records.
[9] 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.