June 15, 2026

TO: Members, Senate Privacy, Digital Technologies and Consumer Protection Committee

SUBJECT: AB 1542 (WARD) SENSITIVE PERSONAL INFORMATION
OPPOSE – AS INTRODUCED JANUARY 5, 2026
SCHEDULED FOR HEARING – JUNE 22, 2026

The California Chamber of Commerce and the undersigned respectfully **OPPOSE AB 1542 (Ward)** as introduced January 5, 2026, because it bans the selling and sharing of sensitive personal information by certain businesses and fails to recognize any legitimate purposes for which an entity covered under the California Consumer Privacy Act (CCPA) should be permitted to disclose sensitive personal information (SPI), even with the consumer's permission. This could result in a host of unintended consequences, including ones that have serious safety implications, such as prohibiting a business from transmitting precise geolocation data *in the event of a car crash*, even if a customer would have allowed them to do so if asked. In particular, such a categorical prohibition risks sweeping in routine and lawful data-sharing practices that underpin modern internet operations, including cloud storage, basic website functionality, security and fraud-prevention activities, and processing under data-processing agreements. In doing so, the bill could not only make it more difficult to prevent fraud, but it could also interfere with the ability of businesses to complete transactions.

And because of the range of data included under SPI, **AB 1542** can also significantly impede the ability of California businesses in arguably "sensitive" sectors to advertise and reach consumers online—the impact of which would be particularly damaging for small and medium businesses, which generally do not have large ad budgets and rely on cost-effective targeted online advertising. For consumers, this means that they would not see as relevant or helpful ads, losing access to the goods and services that they are most likely to find useful or beneficial, including those that they might not otherwise become aware of on their own. Community groups and organizations focused on health and social issues, and political organizations who purchase data from covered businesses may also see a decrease in effectiveness of ads – ultimately interfering with the ability of Californians to connect to the resources they need and political parties from connecting with their voter base.

CCPA was designed to give consumers greater control over their data held by businesses, whereas AB 1542 takes away autonomy and choice

Recognizing the vast amount of personal information in the hands of businesses, the CCPA was intentionally designed to give consumers greater control over their data, applying broadly to online companies, brick and mortar stores, the tech industry or any number of other industries. It was further designed to apply to some businesses based on their annual gross revenue, and others based on their data practices. Across all of these, consumers were to be given the same rights over all their personal information—whether that information was a drivers' license number, their name, their purchase history, their location data, or account info, or other forms of data. Balancing was done over when notices should be given, when there should be an opt-out versus an opt-in, with considerations over things like notice/consent fatigue, but always the point was to put power in the hands of the consumer. Even for teenagers, it was recognized that it was their data, and not the data of their parents and so at certain ages, the decisions belonged to them to make on their own behalf, consistent with other California laws recognizing rights of minors, such as in the medical privacy space.

Indeed, in the Assembly Privacy and Consumer Protection Committee analysis of AB 375 (Chau and Hertzberg, Ch. 55, Stats. 2018), which enacted the landmark privacy legislation, the word "control" was used four times in the first five sentences laying out the purpose of the bill and the author's statement:

> 1) **Purpose of this bill:** This bill seeks to enact the California Consumer Privacy Act of 2018 to further the privacy rights of Californians by providing consumers an effective way to *control* the collection and sale of their PI by businesses, service providers, and third parties. This bill is sponsored by Common Sense Kids Action.
>
> 2) **Author's statement**: According to the author, "Americans value their privacy, be it in the physical world or online. A 2014 PEW Research Center study found that 91% of adults agree that 'consumers have lost *control* over how personal information is collected and used by companies.' A subsequent study in 2016 found that "some 74% say it is 'very important' to them that they be in *control* of who can get information about them, and 65% say it is 'very important' to them to *control* what information is collected about them. […]" [Italics added.]

This bill would for the first time since 2018 take away that control from consumers, abandoning any opt-out or opt-in rights altogether in favor of a complete **ban** on selling or sharing data with third parties, cutting off access to certain information to businesses and consumers entirely.

To the extent that the concern is that bad actors exist that may not adhere to CCPA limits placed on third parties, or that consumers do not know their rights, the answers lie in enforcement and education – not laws that remove consumer choice and substitute regulatory judgment for individuals' discretion over their personal information in the exercise of their personal right of privacy.

CCPA affords consumers strong rights over sensitive PI as amended by voters in Proposition 24

As amended by voters in 2020 by Proposition 24, the CCPA affords Californians significant rights over their sensitive PI (SPI). As a baseline, sensitive PI is subject to the same rights that apply to PI[1] such as the right of deletion or the right to know what information is collected or sold about them. Additionally, in establishing this new category of sensitive PI, Proposition 24 established new, expanded protections that apply solely to SPI. Those protections, collectively, include:

1. **The right to be told at or before the point of collection**, of 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).)

[1] Under the CCPA, PI expressly includes any piece of information that identifies, relates to, describes or is reasonably capable of being associated with, or could reasonably be linked to, directly or indirectly, a particular or person or household. It includes everything from identifiers (such as a person's real name or alias, online identifiers, IP addresses, other similar identifiers), to biometric information and audio, electronic, visual, or similar information; to professional or employment related information, geolocation data, as well as sensitive PI. (Civil Code Sec. 1798.140(v).) In turn, sensitive PI expressly includes "precise geolocation" as well as other forms of information including,[1] among other things, a consumer's:

- social security, driver's license, state identification card, or passport number,
- account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
- racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership;
- contents of their mail, email, and text messages unless the business is the intended recipient of the communication.
- PI collected and analyzed concerning a consumer's health.
- PI collected and analyzed concerning a consumer's sex life or sexual orientation.

2. The right to prevent businesses from collecting or using their SPI for additional purposes that are incompatible with the disclosed purpose for which their SPI was collected absent 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 purpose. (.100(a).)

    - **Third parties** controlling the collection of data about a consumer have an obligation to provide this information "prominently and conspicuously" on the homepage of their internet websites. (.100(b).)

    - Any time a business collects a consumer's data and sells or shares it to a **third party**, or disclose it to a service provider or contractor for a business purpose, they must both specify that the data is sold or disclosed only for limited and specified purposes and impose binding contractual obligations on those entities ***to comply with applicable obligations under the CCPA and provide the same level of privacy protections as required under the CCPA***. (.100(d); again, PI includes SPI.)

4. **The right to direct a business to limit the use and disclosure of SPI to what is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services and to perform specified, limited "business purposes" under the CCPA,** such as security or fraud prevention, as permitted by law [.121; *see* also .140(e)(2)(4)(5) and (8)].

    - Once a consumer exercises this right, the business may not use SPI for any other purpose absent further consent, except as specified. This restriction extends to service providers and contractors once they receive instructions to limit use and disclosure of the consumer's SPI if they have actual knowledge of PI that is SPI.

5. The right to request deletion of any PI that was collected *from* them (.105).

6. 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** (.110 and .115); and the right **opt-out of the sale if the consumer is age 16 or 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).)[2]

With these rights in mind, it is clear that **AB 1542** has overlooked one important mechanism by which it could strengthen consumer protections under the CCPA for sensitive PI *without* removing consumer choice: the opt-in mechanism. An opt-in mechanism for selling or sharing to third parties, unlike a ban, would allow businesses to seek express consent from the consumer, while prohibiting them from selling or sharing to third parties unless the consumer consents, leaving control in the hands of the consumer. Many consumers are already familiar and comfortable with this process for precise geolocation, for example -- turning off location services in their phone and setting it to "unless shared" for certain apps, and deciding yes/no when prompted by the app for certain uses. On the apps they have chosen "never", on occasion they may ask for something and get reminded they cannot have a certain functionality or service because of that choice and can easily go back and change their setting to "unless shared" if they wish. This process provides some balance between consumer privacy with business needs. While we are still evaluating whether this would resolve concerns, a categorical prohibition provides no balance whatsoever.

[2] Additionally, these rights are reinforced by detailed statutory requirements governing notice, disclosure, correction, deletion and mechanisms for opting out or in, or limiting the use of PI or SPI in Sections 1798.130 and 1798.135, as well as preventing any discrimination/retaliation for exercising such rights in 1798.125.

Unintended consequences of AB 1542 – from business, security, public safety, social and political perspectives

While **AB 1542** would continue to permit certain disclosure of sensitive PI to service providers and contractors for permitted business purposes, when it comes to all other persons and entities – "third parties," – the bill would change the law from a "right to limit" model to a categorical prohibition. Again, under the CCPA, a third party is any "person" who is not the business with whom the consumer intentionally interacts and that collects PI (including SPI) from the consumer as a result of that current interaction with the business; a service provider to the business, or a contractor. In turn, a "person" is any individual, company, organization, or "group of persons acting in concert". Thus, in practice, **AB 1542's** ban on selling or sharing sensitive PI with third parties would significantly alter, if not constrain, several common and lawful business operations and even beneficial uses by other third parties—from business to nonprofits, to researchers, to political organizations, and government entities.

- **Impact on certain cross-platform and network-based consumer services.** Many consumer-facing services rely on the ability to share sensitive PI such as precise geolocation or device level signals across multiple independent entities, rather than within a single business-to service provider relationship. For example, fraud prevention tools often rely on signals observed across multiple merchants to detect coordinated attacks and prevent account takeovers; location-based services depend on third party data inputs to provide accurate, real-time recommendations and navigation; and emergency or disaster-response efforts may rely on aggregated mobility data to allocate resources efficiently. Because these use cases inherently involve data sharing across multiple independent entities, they may not fit neatly within service provider or contractor relationships. To the extent **AB 1542** restricts such third party sharing of sensitive PI without clear exceptions, those widely used consumer services could become less effective, leading to increased fraud, reduced service quality, or diminished real-time responsiveness for consumers.

- **Limits on third-party data enrichment and business or government risk management.** Businesses and certain government entities frequently rely on third-party services to enhance their internal data, including for fraud detection and risk assessment and compliance with regulations such as Anti-Money Laundering (AML) or Know Your Customer (KYC). For example, smaller merchants often use third-party networks to verify government-issued identifiers, analyze transaction patterns across multiple businesses, or detect fraudulent activity they could not identify on their own. Similarly, government contractors or verification vendors may rely on shared sensitive PI to ensure public program integrity, prevent fraud, and confirm that benefits reach intended recipients. By restricting the ability to share sensitive PI with these third-party risk and security services, **AB 1542** could leave small businesses and government programs more exposed to identity theft, account abuse, operational disruption, or verification gaps, widening the gap between small entities and larger organizations with in-house capabilities, but harming all organizations in general.

- **Charitable or emergency-response data sharing**: Notably, organizations responding to disasters or coordinating relief efforts often rely on sensitive PI, such as geolocation or household data to allocate resources efficiently and reach those in need. For example, telecom providers, technology platforms, utilities or others may supply data –often in aggregated or pseudonymized form –to public authorities and humanitarian organizations to help map population displacement, prioritize aid delivery, identify vulnerable households and support emergency response, subject to safeguards.

  While de-identification/aggregation data is generally excluded from PI—and therefore deidentified or aggregated forms of SPI would also generally not be PI—it is not difficult to foresee circumstances in emergency response where it might become necessary to share this information in identifiable form. (See Civ. Code 1798.140 (v)(2) and (3) excluding publicly available information as well as deidentified and aggregate consumer information.) Furthermore, SPI is both defined as a category of PI, but it is also defined as an entirely independent term exclusive of PI, where it does not exclude deidentified and aggregate consumer information (see Civ. Code 1798.140(ae)(3)

excluding only publicly available information), creating confusion as to whether or not this data would be excluded when shared with third parties.

Ultimately, in most cases, these nonprofits or government partners are not acting as service providers or contactors for the businesses providing the data. They operate independently to fulfill their public or charitable missions. As such, under **AB 1542's** categorical prohibition, businesses are likely to be restricted from providing this information to some extent, potentially impeding timely relief, limiting the effectiveness of resource allocation or requiring complex contractual arrangements that are impractical in emergency situations.

- **Implications for certain socially beneficial third-party uses**. **AB 1542** does not distinguish between commercial and socially beneficial uses of sensitive PI. For example, it does not provide clear exceptions for the public interest, or academic or research purposes. As a result, nonprofit organizations, academic researchers, and political or community groups could face limitations from receiving sensitive PI, even when their work benefits the public.

    - **Public health research:** nonprofits or universities tracking vaccination coverage or disease outbreaks could face limits on access to precise geolocation or other sensitive data, which may limit their ability to generate timely insights.

    - **Community and political engagement:** local advocacy and voter outreach groups could be limited from targeting constituents in specific areas or evaluating how their ad placements are performing (see below), which may reduce the efficacy of outreach and engagement programs. This is particularly true for those community groups and organizations focused on health and social issues, including affinity groups and support groups relating to health and sexual identity, immigration or civil rights organizations, or religious organizations, based on the definition of sensitive PI including:

        - a consumer's racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership.

        - PI collected and analyzed concerning a consumer's health.

        - PI collected and analyzed concerning a consumer's sex life or sexual orientation.

- **Third party advertising models - placing small businesses and startups at a relative disadvantage.** While advertising, on the whole, remains permissible, **AB 1542** may increase costs and reduce access to certain targeted advertising tools that rely on sensitive PI, particularly for smaller businesses and startups that lack the large first-party datasets of larger competitors. Smaller entities often rely on third-party platforms that use data such as geolocation to reach local customers. This first-party data asymmetry or imbalance may further widen existing gaps between smaller businesses and larger incumbents with first-party data and in-house analytics.

- **Places constraints on independent measurement, putting all businesses in the position of relying on limited data to understand if their advertising dollars are properly allocated. For small and medium sized businesses, as well as other entities, these dollars are limited, and independent verification is particularly critical.** Businesses and other entities often depend on neutral, third-party providers to measure the effectiveness of advertising or other initiatives, whether for commercial or political purposes. For instance, a small local clothing store runs an online ad and wants to know, "did people who saw this ad actually walk into my store?" To do this, the store may use an independent provider to determine whether a digital advertising campaign resulted in in-store visits using precise geolocation signals, comparing the people who saw the ad with the people who physically visited the shop using precise geolocation signals. Under **AB 1542**, if that provider is considered a third party, the use of sensitive PI for this purpose would be restricted, effectively ending independent verification. For small and medium-sized businesses, this is particularly problematic, as they are forced to rely on the self-reported metrics of the platforms they

place ads with and have small ad-spend to begin with if they get it wrong. It is easy to envision this also being very problematic in other contexts, such as political campaigns.

Recent legislation demonstrates there are more narrow public policy options to address concerns

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. Of course, one approach would be to transition from an opt-out mechanism for sensitive PI, to an opt-in. But we also note that this is not the first time the Legislature has grappled with these concerns post-CCPA.

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 protection 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 protection for Californians to keep data from being transferred to certain entities.

For these reasons we must **OPPOSE AB 1542 (Ward).**

Sincerely,

Ronak Daylami
Vice President for Advocacy | Privacy, Cybersecurity & Emerging Technologies
on behalf of

American Property Casualty Association, Laura Curtis
Association of National Advertisers, Christopher Oswald
California Chamber of Commerce, Ronak Daylami
California's Credit Unions, Eileen Ricker
California Retailers Association, Jacob Brint
Civil Justice Association of California, Annalee Augustine
Computer & Communications Industry Association, Aodhan Downey
Internet.Works, Austin Heyworth
Insights Association, Howard Fienberg
Software Information Industry Association, Abigail Wilson
TechNet, Robert Boykin

cc: Legislative Affairs, Office of the Governor
Charles Loudon, Office of Assemblymember Ward
Christian Kurpiewski, Chief Consultant, Senate Privacy, Digital Technologies & Consumer Protection Committee
Emilye Reeb, Consultant, Senate Republican Caucus

RD:ldl