March 11, 2025

TO: Members, Assembly Privacy and Consumer Protection Committee

SUBJECT: AB 566 (LOWENTHAL) CALIFORNIA CONSUMER PRIVACY ACT OF 2018: OPT-OUT PREFERENCE SIGNAL
OPPOSE – AS INTRODUCED FEBRUARY 12, 2025
SCHEDULED FOR HEARING – MARCH 18, 2025

The California Chamber of Commerce and the undersigned respectfully **OPPOSE AB 566 (Lowenthal),** which effectively makes universal opt-out preference mechanisms mandatory under the California Consumer Privacy Act (CCPA) to transmit consumers' opt-out preferences to businesses that they interact with online. We support user choice, which is why browsers and mobile operating systems already compete on offering clear, effective user controls over data uses. Users also can choose apps or extensions to manage their privacy preferences in a centralized manner. However, whereas online services and advertisers can and do distinguish data uses by jurisdiction—including for California users—mobile operating systems and software are offered globally to billions of users and cannot be easily altered for California users alone.

Universal opt-out preference mechanisms (also called global privacy controls) raise several important policy questions: what exactly does a global privacy control mean exactly when different states are proposing different opt-outs? Do businesses need to have different controls for every state/jurisdiction, or each different mechanism? How should users expect the mechanism to work in relation to their online service controls that may differ or conflict? How are businesses expected to handle conflicting signals? Ultimately, these opt-out preference mechanisms are not yet ripe to consider as a mobile operating system- or browser-mandated option and **AB 566** would merely expand Agency authority to the detriment of consumers and businesses alike.

Whereas Proposition 24 recognized the complexity of implementing opt-out preference signals and made the adoption of the signals optional, AB 566 appears to prioritize efficiency and consolidation of user choices above all else – even informed consent

First and foremost, it is important to know that voters already allowed for businesses to incorporate and recognize opt-out preference signals under the CCPA when they passed Proposition 24. However, in contrast to **AB 566**, Proposition 24 does not actually mandate businesses to provide a global opt-out signal; instead, it provides businesses the option and required the California Privacy Protection Agency (hereinafter, "Privacy Agency" or "Agency") to adopt regulations around that voluntary use.

Specifically, voters provided businesses three options for implementing a consumer's "opt-out" requests via subdivisions (a) and (b) of Section 1798.135 of the Civil Code:

- First, a business has the option to have one "Do Not Sell or Share My Personal Information" link as well as a separate "Limit the Use of my Sensitive Personal Information" link.
- Second, they have the option to have a single link that does both.
- Alternatively, the third option is to not have any links, as long as they recognize an opt-out preference signal.

In taking this multi-pronged, flexible approach, voters provided businesses the opportunity to implement the most effective method for their situation, while still enabling consumers to effectuate their opt-out rights. And in direct contrast to **AB 566**, voters recognized the complexity of implementing an opt-out preference signal when they directed the Agency to adopt regulations that would ensure that the requirements and specifications for the opt-out preference signal, among other things, are free of defaults that presuppose consumer intent and clearly described and easy to use, and not conflict with other commonly used privacy settings or tools that consumers may employ. (Section 1798.185(a)(19).)

AB 566 will upend this flexible and balanced approach taken by voters and yet fails to account for any of the myriad issues raised by mandating global privacy controls. For example, it does not permit consumers to reverse their decision and opt-back in if they so choose, both as a general matter and for specific use cases for specific businesses as well. Nor does it provide any clarity on how businesses can provide consumers who have previously indicated they wish to opt out via the signal with the opportunity to consent to the sale and sharing of their PI or the use and disclosure of their sensitive PI with that business, specifically. It also fails to ensure that opt-out signals avoid default settings and or to promote informed choices about how they interact with applications and websites by authorizing businesses to notify consumers of both the benefits and consequences of opting-out and the use of cookies. In this way, **AB 566** appears to prioritize efficiency and consolidation of user choices above all else.

Serious ambiguities persist under AB 566 and the Privacy Agency continues to seek carte blanche authority

AB 566 sets forth that "a business shall not develop or maintain a browser that does not include a setting that enables a consumer to send an opt-out preference signal to businesses with which the consumer interacts through the browser." First, there are significant ambiguities here that could mislead consumers in significant ways. Take into consider, for example, the scope of businesses to which the bill applies – it is still unclear whether **AB 566** will only impact those entities subject to the CCPA. Without additional clarity, California consumers could very well be duped into thinking that their privacy is protected across the internet and mobile ecosystem, when in fact there are a large number of entities they might interact with that are not subject to the CCPA, and can legally ignore the signal or treat it as something different.

Second, it is unclear why the bill precludes developing or maintaining such a browser, as opposed to making it available for use by consumers. Third, insofar as the bill requires that the required setting be "easy to locate and configure" for "a reasonable person", it fails to provide sufficient clarity as to what is considered "easy" to locate and configure or distinguish how a "reasonable person" differs from an "average consumer." What is considered "easy" for the "reasonable person" of one generation or for a native English speaker is not necessarily "easy" for others. And how would the reasonable person standard (which is ordinarily found in negligence laws) differ from the "average consumer" standard which is the standard relied upon elsewhere in the CCPA?[1]

Furthermore, is unclear how the "mobile operating systems" provisions are ultimately envisioned to work. If a consumer enables an opt out on a phone, does that mean they have automatically opted out of targeted ads for every single business whose app is on the phone? The consumer would likely not understand the implications. To give the Privacy Agency such carte blanch authority is short sighted and not how public policy should be made – the Legislature should set statutory rules based on existing technologies and providing clear parameters around any necessarily implementing regulations to be issued by the Agency.

Finally, the bill prohibits a business from developing or maintaining a browser that does not include a setting that enables a consumer to send out an opt-out preference signal, "unless otherwise prohibited by federal law". It is unclear what this statement is seeking to accomplish or if this is merely a drafting error (*e.g.,* compare this to a statement that instead provides that businesses are prohibited from developing such browsers "unless otherwise required by federal law"). It arguably appears to suggest that that a global opt

[1] *See* Civ. Code Sec. 1798.185(a)(5) requiring the Agency to adopt rules, procedures, and any exceptions necessary to ensure that notices and information that businesses are required to provide are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, [and] are available in the language primarily used to interact with the consumer…".)

out signal is mandatory unless a federal law is passed preempting the state from making it so—even though the statute passed by voters reflects that it is optional.

AB 566 creates significant compliance questions for businesses operating in multiple jurisdictions

Many jurisdictions around the world are issuing similar laws and regulations to adopt their own opt-out signal requirements (*e.g.,* Colorado or Connecticut). Colorado's privacy law, for example, wisely requires clear communication of a consumer's "affirmative, freely given, and unambiguous choice to opt out" but also prohibits their rule from adopting a mechanism that is a default setting and requires that the signal permit the controller to accurately authenticate the consumer as a resident of the state and determine that the mechanism represents a legitimate request to opt-out. Lack of harmonization and consistency with such rules cropping up in other states is extremely problematic.

Because the scope of universal opt-out preference mechanisms is inconsistent across other jurisdictions, it is unclear how a user agent (*i.e.,* a software agent responsible for retrieving and facilitating end-user interaction with web content) such as a browser or operating system can or should properly communicate an opt-out preference signal in a way that is made clear to a consumer. And since the scope of the mechanism could change within the same jurisdiction over time, or over several jurisdictions, it will be impossible to communicate to the user what their choice affects and how changes by geography and time would affect their digital experience, not to mention unreasonably burdensome. As the scope of an opt-out mechanism's effect changes, the browser our other user agent would have to regularly request another consent from the user, and to explain to the user why they were asking for consent again, and what effect the change would have.

AB 566 ignores the complexities and challenges involved in mandating global privacy controls and raises significant implementation issues

In addition to problems and ambiguities highlighted above, it is unclear how an opt-out mechanism browser setting would need to intersect with other privacy related user settings which control similar functionality, and which a user has interacted with (e.g., Google privacy settings, iOS privacy settings, AdChoices), or how those settings may override a universal opt-out signal setting depending on the jurisdiction.

Requiring that user agents such as browsers and operating systems send opt-out preference signals downstream to other parties will also be complicated, as each browser or operating system would be required to communicate the opt-out mechanism choice in exactly the same way, using exactly the same user experience. This will require more than standardization of universal opt-out mechanism interfaces: it will require other aspects of browser or operating system settings to also be designed in the same way, to support common interfaces. Such requirements will reduce innovation and differentiation amongst competitors. It could potentially also impact how existing privacy tools available to consumers as apps or extensions operate and require that such services likewise be re-engineered to address evolving requirements.

And while a browser might transmit a user's choice downstream to receiving entities, it would be almost impossible for it to enforce compliance with the user's signal. As a technical matter, a business further downstream may not be able to recognize a user from a browser signal, which is why signals should only apply to recognized identifiable consumers in order to avoid the risk of a choice only being recognized on an individual browser. Technical standards are also needed to ensure that the signal accurately identifies the residency of the consumer,[2] so the business knows that the user is exercising an opt-out choice under the CCPA. Nonetheless, in cases of non-compliance, the consumer would almost certainly either be confused or hold the browser responsible for downstream partners' lack of compliance. This misunderstanding of responsibility will unnecessarily erode consumer trust in browsers and operating systems.

[2] Of course, businesses should not be required to identify unauthenticated users to ensure that they are opted out of all forms of selling or sharing PI. The CCPA specifically states under Section 1798.145(j) that the act shall not require reidentifying or otherwise linking information that "in the ordinary course of business, is not maintained in a manner that would be considered [PI]."

And finally, we are concerned over the possibility that consumers may send conflicting signals which would create significant compliance burdens for businesses. The risk includes a scenario where a consumer uses a universal opt-out but then requests a specific site or app to override, or requests to opt-in for a specific service. It will be complicated for browsers to maintain a list of what sites or apps are, and are not, allowed to send and receive data.

Governor's veto message of AB 3048 last year clearly shared many of these concerns

Last year, the Governor vetoed a virtually identical bill in AB 3048 (Lowenthal), stating that despite sharing a desire to enhance consumer privacy, he is concerned "about placing a mandate on operating system (OS) developers at this time. No major mobile OS incorporates an option for an opt-out signal. By contrast, most internet browsers either include such an option or, if users choose, they can download a plug-in with the same functionality. To ensure the ongoing usability of mobile devices, it's best if design questions are first addressed by developers, rather than by regulators." We do not believe anything has changed since the Governor's veto on September 20, 2024, that would warrant passage of the same public policy today.

Regardless, voters were very clear when they passed Proposition 24 that consumers should be given choices. The Agency should focus on effectuating Proposition 24 to ensure voters are given the choices that voters demanded, instead of seeking carte blanch authority so they can rewrite the law as they see fit or retroactively authorizing their prior regulations that clearly went far beyond their existing scope of authority.

For all the aforementioned reasons, we must **OPPOSE AB 566 (Lowenthal).**

Sincerely,

Ronak Daylami
Policy Advocate
on behalf of

Association of National Advertisers, Christopher Oswald
California Chamber of Commerce, Ronak Daylami
California Retailers Association, Ryan Allain
Computer & Communications Industry Association (CCIA), Aodhan Downey
Insights Association, Howard Fienberg
Software Information Industry Association, Abigail Wilson
TechNet, Jose Torres

cc: Legislative Affairs, Office of the Governor
Consultant, Assembly Privacy and Consumer Protection Committee
Jacqueline Anapolsky, Office of Assemblymember Lowenthal
Liz Enea, Consultant, Assembly Republican Caucus

RD:ldl