September 6, 2024

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

SUBJECT: AB 3048 (LOWENTHAL) CALIFORNIA CONSUMER PRIVACY ACT OF 2018: OPT-OUT PREFERENCE SIGNAL
REQUEST FOR VETO

Dear Governor Newsom:

The California Chamber of Commerce and the undersigned respectfully urge you to **VETO AB 3048 (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, yet, **AB 3048** appears to prioritize efficiency and consolidation of user choices above all else – even above consumer privacy.

Proposition 24 recognized the complexity of implementing opt-out preference signals and made the adoption of the signals optional, whereas AB 3048 removes necessary flexibility

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 3048**, Proposition 24 does not actually mandate businesses to provide a global opt-out signal; it provides businesses the option and requires regulations around that voluntary use.

Specifically, subdivisions (a) and (b) of Section 1798.135 of the Civil Code gives businesses three options for implementing a consumer's "opt-out" requests. A business can 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 or they can 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. This allows businesses the opportunity to implement the most effective method for their particular situation, while still providing individuals the opportunity to opt-out of the use of their PI.

To effectuate these provisions, voters also instructed the Agency to adopt regulations "to define the requirements and technical specifications for an opt-out preference signal sent by a platform, technology, or mechanism, to indicate a consumer's intent to opt out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information." In direct contrast to **AB 3048**, Proposition 24 also recognized the complexity of implementing an opt-out preference signal, instructing the Agency to ensure that the requirements and specifications for the opt-out preference signal, among other things, be 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 3048 upends the balanced approach taken by voters, removing any such flexibility in the law. Yet it does not 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 3048** appears to prioritize efficiency and consolidation of user choices above all else, including consumer privacy.

Serious ambiguities persist under AB 3048 and the Privacy Agency continues to seek carte blanche authority

AB 3048 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." While we appreciate recent amendments which clarify what exactly it is that the consumer is opting out of other ambiguities remain. First, with respect to the scope of businesses to which the bill applies – it is still unclear whether AB 3048 will only impact those entities subject to the CCPA. Without additional clarity, California consumers could still 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 use", it fails to provide any clarity as to what is considered easy to locate and use. Do businesses have to ensure that it is easy to locate and use by any individual user with individual needs and challenges? Or the average user?

Next, Senate amendments replace references to "devices" with "mobile operating systems" and make the application to mobile operating systems operative only upon adoption of regulations by the California Privacy Protection Agency that outline the requirements and technical specifications for an opt-out preference signals to be used by a mobile operating system. It is unclear how this is 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 be setting the direction and parameters of any regulations to be issued by the Agency.

Finally, recent amendments specify that 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").

AB 3048 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 3048 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,[1] 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

[1] 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]."

misunderstanding of responsibility will unnecessarily erode consumer trust in browsers and operating systems.

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.

For all the aforementioned reasons, we request that you **VETO AB 3048 (Lowenthal)**.

Sincerely,

Ronak Daylami
Policy Advocate
on behalf of

American Association of Advertising Agencies (4A's)
Association of National Advertisers
California Chamber Commerce
California Land Title Association
California Mortgage Bankers Association
California Retailers Association
Civil Justice Association of California
Computer and Communications Industry Association
Insights Association
Internet Coalition
Los Angeles Area Chamber of Commerce
TechNet