March 26, 2024

Chair Rebecca Bauer-Kahan
Vice Chair Joe Patterson
Committee on Privacy and Consumer Protection
California Assembly
Legislative Office Building
1020 N Street, Room 162
Sacramento, CA 95814

Re: AB 3048 (Lowenthal) – *SUPPORT*

Dear Chair Bauer-Kahan and Vice Chair Patterson,

The undersigned organizations and individuals write in strong support of AB 3048, a bill that would require browsers and devices to include a setting that enables a consumer to send an opt-out preference signal. While California consumers enjoy the right to send legally binding opt-out preference signals, major browsers like Chrome, Safari, and Edge, as well as the Android and iOS mobile platforms, have suppressed usage of this right by denying native opt-out preference signal functionality. This bill is vital to ensure that millions of Californians have a practical way to manage their privacy choices under the CCPA.

The CCPA made California the first state in the nation to require that covered businesses respond to opt-out preference signals, which a consumer may send via a "platform, technology, or mechanism."[1] When enabled, the signal automatically communicates the consumer's preference to opt-out of the sale or sharing of their personal information by each business with which the consumer interacts online.

---

[1] CCPA Sec. 1798.135(b)(1)

Opt-out preference signals were a policy response to the suboptimal consumer rights formulation under the initial version of the CCPA, which required consumers to effectuate their opt-out requests individually with each business with which they interacted. That meant that consumers with a generalized preference not to allow the sharing or selling of their personal information would have had to contact hundreds, if not thousands, of businesses in order to satisfy that preference.

As Consumer Reports testing showed,[2] the individual opt-out structure is intensely cumbersome for consumers – many consumers struggled to complete an opt-out request on just a single data broker's website – an arrangement that depresses the usage of consumer rights under the law. Opt-out preference signals were intended to relieve this burden and make it easier for consumers to express their privacy preferences.

Subsequent to the passage of CPRA's amendments to the CCPA that created the opt-out preference signal requirement (as well the enactment of several other state privacy laws that create similar requirements),[3] we've seen numerous privacy-conscious browser vendors, such as Brave, DuckDuckGo, and Firefox support the concept of opt-out preference signals. Most commonly, such browsers do so by enabling usage of Global Privacy Control,[4] a technical specification that has been interpreted by the California Privacy Protection Agency [5] and California Attorney General [6] to serve as a permissible opt-out preference signal under the CCPA. These browsers typically either enable the GPC signal to be sent by default or make it a setting the user can easily toggle on or off.

However, the largest browser vendors (Apple Safari, Google Chrome, and Microsoft Edge, which cumulatively enjoy more than 90% of the browser share in the United States) currently do not provide native support for opt-out preference signals.[7] Similarly, mobile platforms, which use the same HTTP standard as web browsers and could implement GPC with little effort, do not support it. Today, if a user wants to send an opt-out preference signal on Chrome, Safari, or Edge, they need to download a third-party extension to do so, while a mobile platform user cannot configure their device to send an opt-out preference signal at all. As a result, millions of Californians, while technically enjoying the right to send such a signal, likely have no idea that this right even exists and have no easy way of acting on it even if they did.

---

[2] Maureen Mahoney, California Consumer Privacy Act: Are Consumers' Rights Protected, Consumer Reports (Oct.
1, 2020),
https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf2.pdf

[3] Universal opt-out provisions are included in the California, Connecticut, Colorado, Delaware, New Hampshire, New Jersey, Montana, Oregon and Texas comprehensive privacy laws.

[4] https://globalprivacycontrol.org/

[5] Frequently Asked Questions, California Privacy Protection Agency, at 8. How to Submit Requests, https://cppa.ca.gov/faq.html.

[6] Archive - Attorney General Becerra, Twitter.com, Jan. 28, 2021, https://twitter.com/AGBecerra/status/1354850758236102656.

[7] United States Browsers Market Share, (February 2024), https://www.similarweb.com/browsers/united-states/

Browser and platform vendors could easily add universal opt-out functionality to their products. In 2011, in response to urging from the Federal Trade Commission, all major browsers added an option to send "Do Not Track" signals within a matter of months, despite the fact that "Do Not Track" had no clear meaning or legal effect. Compliance with universal opt-out mechanisms, on the other hand, is currently mandated by California and will soon be mandated by at least eight other state privacy laws in the coming years (with more likely to be passed in the near future).

AB 3048 will ensure that consumers have the ability to use their privacy rights by requiring that browser vendors and suppliers of devices (for example, a mobile device or "smart" TV) include an easy to locate and use setting that enables the consumer to send an opt-out preference signal. This bill's approach will help reduce opt-out friction and make it easier for California residents to control their data, while also providing for flexibility by allowing the CPPA to adopt rules that will allow the law to keep pace with technology.

For the reasons listed above, we are proud to support AB 3048 and urge the Legislature to pass it.

Sincerely,

Accountable Tech
Brave Software
California Public Interest Research Group (CALPIRG)
Center for Democracy & Technology
Center for Digital Democracy
Consumer Federation of America
Consumer Reports
Digital Content Next
Electronic Privacy Information Center (EPIC)
Privacy Rights Clearinghouse
Don Marti, VP of Ecosystem Innovation, Raptive
Robin Berjon, Governance & Standards, Protocol Labs; IPFS Steering Committee; Board Director, W3C
Sebastian Zimmeck, Assistant Professor of Computer Science, Wesleyan University

cc: The Honorable Members of the Assembly Committee on Privacy & Consumer Protection
        Julie Salley, Chief Consultant
        Assemblymember Josh Lownethal