Date of Hearing: April 1, 2025
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 566 (Lowenthal) – As Introduced February 12, 2025

PROPOSED AMENDMENTS

SUBJECT: California Consumer Privacy Act of 2018: opt-out preference signal

SYNOPSIS

"The right of privacy is an important American heritage and essential to the fundamental rights guaranteed by the First, Third, Fourth, Fifth and Ninth Amendments to the U.S. Constitution. This right should be abridged only when there is compelling public need. Some information may remain as designated public records but only when the availability of such information is clearly in the public interest."

– Ballot statement
California Proposition 11: Right of Privacy (1972)

Contrary to the privacy that Californians were promised with the passage of Proposition 11 in 1972, Californians are constantly tracked, monitored, and surveilled, both in their own homes and out in public. Virtually every detail of our lives are being commodified: what we read, what websites we visit, whether we are married and have children, our educational level and income bracket, our location, our purchasing habits, our personal interests, our physical fitness, our gender, who our intimate partners are, our health conditions and our religious faith. Technology companies track what we do on and off their platforms, often combining their own information with enormous datasets purchased through the largely unregulated consumer data market.[1]

This bill, sponsored by the California Privacy Protection Agency and virtually identical to last year's AB 3048 (Lowenthal), attempts to give Californians a tool to limit the sharing and sale of their personal information. It requires that internet browsers and mobile operating systems on smartphones and tablets include an opt-out preference signal allowing consumers interacting with businesses online to automatically exercise their right to opt out of the selling and sharing of their personal information. The Committee has proposed two amendments in Comment #6. The substantive amendment removes language stating the agency may update the bill's definitions of "browser" and "mobile operating systems" while retaining the agency's authority to adopt regulations and necessary to implement the bill. The second amendment is non-substantive and technical in nature.

Along with the sponsor, Consumer Reports, Mozilla, Brave Software, and several other privacy and consumer advocacy organizations support this bill. The California Chamber of Commerce, Tech Net and a number of business and technology associations oppose.

THIS BILL:

---

[1] *A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services.* "Preface" by Samuel Levine, Director, Bureau of Consumer Protection, Federal Trade Commission (September 2024) https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf.

1) Prohibits a business from developing or maintaining a browser or mobile operating system that does not include a setting that enables consumers to send an opt-out preference signal to other businesses that the consumer interacts with through the browser.

2) Requires that the opt-out preference signal on a browser be easy for a reasonable person to locate and configure.

3) Delays implementation of the mobile operating system requirements until six months after the adoption of regulations by the California Privacy Protection Agency (CPPA).

4) Defines "browser" to mean an interactive software application that is primarily used by a consumer to access websites on the internet.

5) Defines "mobile operating system" to mean an operating system in use on a smartphone or tablet.

6) Defines "opt-out preference signal" to mean a signal that complies with the requirements of this legislation and communicates the consumer's choice to opt out of the sale and sharing of the consumer's personal information.

7) Authorizes the California Privacy Protection Agency to use its regulatory process to change the statutory definition of "browser" and "mobile operating system" in order to address changes in technology, data collection, obstacles to implementation or privacy concerns.

EXISTING LAW:

1) Provides, pursuant to the California Constitution, that all people are by nature free and independent and have inalienable rights. Among these is the fundamental right to privacy. (Cal. Const. art. I, § 1.)

2) States that the "right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them." Further states these findings of the Legislature:

    a) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies.

    b) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.

    c) In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits. (Civ. Code § 1798.1.)

3) Establishes the California Consumer Privacy Act (CCPA). (Civ. Code §§ 1798.100-1798.199.100.)

4) Prohibits a business from selling or sharing the personal information of a child that is 16 years of age or younger, if the business has actual knowledge of the child's age, unless the

child, or the child's parent or guardian in the case of children less than 13 years old has affirmatively authorized the sharing of selling of the personal information. (Civ. Code § 1798.120(c).)

5) Provides a consumer, subject to exemptions and qualifications, various rights, including the following:

   a) The right to know the business or commercial purpose for collecting, selling, or sharing personal information and the categories of persons to whom the business discloses personal information. (Civ. Code § 1798.110.)

   b) The right to request that a business disclose the specific pieces of information the business has collected about the consumer, and the categories of third parties to whom the personal information was disclosed. (Civ. Code § 1798.110.)

   c) The right to request deletion of personal information that a business has collected from the consumer. (Civ. Code § 1798.105.)

   d) The right to opt-out of the sale of the consumer's personal information if the consumer is over 16 years of age. (Sale of the personal information of a consumer below the age of 16 is barred unless the minor opts-in to its sale.) (Civ. Code § 1798.12.)

   e) The right to direct a business that collects sensitive personal information about the consumer to limit its use of that information to specified necessary uses. (Civ. Code § 1798.121.)

   f) The right to equal service and price, despite the consumer's exercise of any of these rights, unless the difference in price is reasonably related to the value of the customer's data. (Civ. Code § 1798.125.)

6) Requires a business to provide clear and conspicuous links on its homepage allowing consumers to opt-out of the sale or sharing of their personal information and use or disclosure of their sensitive personal information. (Civ. Code § 1798.135(a).)

7) Allows a business to not comply with the requirement to provide opt-out links if the business allows consumers to opt-out of the sale, sharing, and use of their information through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism based on the technical specifications set forth in the Privacy Agency's regulations. (Civ. Code § 1798.135(b).)

8) Establishes the California Privacy Protection Agency (Privacy Agency), vested with full administrative power, authority, and jurisdiction to implement and enforce the CCPA. The Privacy Agency is governed by a five-member board, with the chairperson and one member appointed by the Governor, and the three remaining members are appointed by the Attorney General, the Senate Rules Committee, and the Speaker of the Assembly. (Civ. Code § 1798.199.10.)

9) Requires the Privacy Agency to issue regulations that:

a) 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.

b) Establish technical specifications for an opt-out preference signal that allows the consumer, or the consumer's parent or guardian, to specify that the consumer is less than 13 years of age or at least 13 years of age and less than 16 years of age. (Civ. Code § 1798.185.)

10) Defines the following terms under the CCPA:

a) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes such information as:

i) Name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other identifier.

ii) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

iii) Biometric information.

iv) Internet activity information, including browsing history and search history.

v) Geolocation data.

vi) Audio, electronic, visual, thermal, olfactory, or similar information.

vii) Professional or employment-related information. (Civ. Code § 1798.140(v).)

b) "Sensitive personal information" means personal information that reveals a person's:

i) Social security, driver's license, state identification card, or passport number.

ii) Account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials.

iii) Precise geolocation.

iv) Racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership.

v) Email, mail and text messages.

vi) Genetic data.

vii) Information collected and analyzed relating to health.

viii) Information concerning sex life or sexual orientation. (Civ. Code § 1798.140(ae).)

COMMENTS:

1) **Author's statement**. According to the author:

> Californians have the right to easily opt-out of the sale of their personal information through opt-out preference signals, yet a significant number of leading web browsers do not offer such signals. Consumers are often unaware of how their data is being collected and shared when they are using the internet, which leads to the misuse of their personal data.
>
> AB 566 makes it easier for consumers to state their privacy preferences from the start by requiring web browsers to allow a user to exercise their opt-out rights at all businesses with which they interact online in a single step.

2) **Surveillance capitalism.** For almost 20 years experts have been warning us about the erosion of our private lives. They note that this erosion is happening one small bit at a time, likely without people even noticing. With the advent of the internet and advances in technology, it is no longer easy for people to decide which aspects of their lives should be publicly disclosed. As Alex Preston noted in *The Guardian* a decade ago:

> We have come to the end of privacy; our private lives, as our grandparents would have recognised them, have been winnowed away to the realm of the shameful and secret. . . . Insidiously, through small concessions that only mounted up over time, we have signed away rights and privileges that other generations fought for, undermining the very cornerstones of our personalities in the process. While outposts of civilisation fight pyrrhic battles, unplugging themselves from the web. . . the rest of us have come to accept that the majority of our social, financial and even sexual interactions take place over the internet and that someone, somewhere, whether state, press or corporation, is watching.[2]

Since the time this piece was published, it has become increasingly clear that not only has our right to privacy significantly eroded, but our private information and activities are now being harvested and sold for a profit. This commodification of personal information has been dubbed "surveillance capitalism" by social psychologist Shoshana Zuboff. In an opinion piece for *The New York Times*, in 2021, Dr. Zuboff warned:

> As we move into the third decade of the 21st century, surveillance capitalism is the dominant economic institution of our time. In the absence of countervailing law, this system successfully mediates nearly every aspect of human engagement with digital information. The promise of the surveillance dividend now draws surveillance economics into the "normal" economy, from insurance, retail, banking and finance to agriculture, automobiles, education, health care and more. . . .
>
> An economic order founded on the secret massive-scale extraction of human data assumes the destruction of privacy as a nonnegotiable condition of its business operations. With

---

[2] Preston, Alex. "The death of privacy." *The Guardian* (Aug. 3, 2014) https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston.

> privacy out of the way, ill-gotten human data are concentrated within private corporations, where they are claimed as corporate assets to be deployed at will.[3]

The slow erosion of privacy, through the collection of what seem to be relatively small pieces of personal information may not cause people to be overly concerned. However, the private information being amassed on everyone in the United States that is being made available to individuals, private companies, and local, state, and federal government agencies should alarm everyone. University of Virginia Law Professor Danielle Citron warned in an interview with *The Guardian* in 2022, "We don't viscerally appreciate the ways in which companies and governments surveil our lives by amassing intimate information about our bodies, our health, our closest relationships, our sexual activities and our innermost thoughts. Companies are selling this information to data brokers, who are compiling dossiers with about 3,000 data points on each of us."[4]

With the rapid growth in the development of Artificial Intelligence (AI) systems, particularly large-language models, people's personal information has become even more valuable as developers require ever-increasing amounts of data to train their foundation models. Going forward, AI development will continue to increase developers' hunger for training data, fueling an even greater race for data acquisition than we have already seen in past decades.[5]

3) **Why protecting personal information is important**. Some may consider sharing their private information, including websites they visit, purchases, employment history, menstrual cycles, name, pictures, locations and movements, social media posts and reactions, and other seemingly innocuous information a reasonable price to pay for freely accessing the internet. However, failing to actively protect our private information can have real world consequences. As an example, dating app, Grindr, was fined 10 percent of its global annual revenue by the Norwegian Data Protection Authority in 2021 for sharing deeply personal information with advertisers, including location, sexual orientation and mental health details.[6] This was not the first time Grindr had failed to protect their users' private information. Several years earlier, it was revealed that the company had shared HIV status and the location data from their users with two companies who were contracted to optimize the Grindr platform.[7]

Catherine Powell in a 2023 blog post for the *Council on Foreign Affairs* highlights the ubiquitous plundering of people's personal, intimate data:

> If you've engaged with any form of technology recently—whether through a smartphone, social media, a fitness tracker, even a seemingly innocuous game like Candy Crush—you

---

[3] Zuboff, Shoshana. "You Are the Object of a Secret Extraction Operation." *The New York Times* (Nov. 12, 2021) https://www.nytimes.com/2021/11/12/opinion/facebook-privacy.html.
[4] Clarke, Laurie. "Interview - Law professor Danielle Citron: 'Privacy is essential to human flourishing,'" *The Guardian* (Oct. 2, 2022) https://www.theguardian.com/technology/2022/oct/02/danielle-citron-privacy-is-essential-to-human-flourishing.
[5] King, Jennifer and Meinhardt, Caroline. *Rethinking Privacy in the AI Era*. Human-Cantered Artificial Intelligence at Stanford University (Feb. 2024) https://hai-production.s3.amazonaws.com/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf.
[6] Hern, Alex. "Grindr fined £8.6m in Norway over sharing personal information," *The Guardian* (Jan. 26, 2021) https://www.theguardian.com/technology/2021/jan/26/grindr-fined-norway-sharing-personal-information.
[7] "Grindr shared information about users' HIV status with third parties." *The Guardian* (Apr. 3, 2018) https://www.theguardian.com/technology/2018/apr/03/grindr-shared-information-about-users-hiv-status-with-third-parties.

> have accumulated a substantial amount of intimate privacy data. Intimate data ranges from your location, to when you fall asleep, to even more closely guarded information like your menstrual cycle or sexual partners. And every day, this data is scraped, bought, and sold by data brokers to third parties. Beyond violating our privacy, this repurposing of our personal data undermines our security.[8]

4) **Challenges with California's privacy laws.** In 1972, at the Legislature's urging, the people of California used the initiative process to add "privacy" to the list of "inalienable rights" in the state constitution.[9] Proponents noted the initiative was specifically designed to preserve Californians' private lives and fundamental rights in the face of technological advances. They argued: "The right of privacy is the right to be left alone. . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes. . . ."[10]

In 2018, the Legislature enacted the California Consumer Privacy Act (CCPA)(AB 375 (Chau, Chap. 55, Stats. 2018)), which gave consumers certain rights regarding their personal information,[11] such as the right to: (1) know what personal categories of information about them are collected and sold; (2) request the deletion of personal information; and (3) opt-out of the sale of their personal information, or opt in, in the case of minors under 16 years of age.

Subsequently, in 2020, California voters passed Proposition 24, the California Privacy Rights Act (CPRA), which established additional privacy rights for Californians. Chief among these rights was the right of a consumer to limit a business's use of sensitive personal.[12] With the passage of the CCPA and the CPRA, California, at the time, had the most comprehensive laws in the country when it came to protecting consumers' rights to privacy.

Since the passage of the CCPA, 19 additional states have passed comprehensive privacy laws. Of those states, 17 have laws that are more privacy protective. 16 states require consumers to "opt in" to the sharing and sale of sensitive information and one state, Maryland, prohibits the sharing of sensitive information entirely.[13] In the states that have come after California, privacy is the default. The CCPA, on the other hand, relies on consumers actively exercising their rights to "opt out" of the sharing and sale of their personal information and the sharing, sale and use of their sensitive personal information. The challenge is that in order to exercise those rights, consumers must first find the businesses that have collected their personal information and then find a way to contact the company to exercise those rights. It is likely that the average consumer often does not even realize that their personal information is being harvested, used to micro target them for advertising, and sold as a commodity to other companies.

---

[8] Powell, Catherine. "Data is the New Gold, But May Threaten Democracy and Dignity," *Council on Foreign Relations* (Jan. 5, 2023) https://www.cfr.org/blog/data-new-gold-may-threaten-democracy-and-dignity-0.
[9] California Proposition 11 (1972), "Constitutional Right to Privacy Amendment."
[10] *Right of Privacy California Proposition 11*, UC L. SF SCHOLARSHIP REPOSITORY (1972), pp. 26–27, https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props.
[11] Civ. Code § 1798.140(v). See **EXISTING LAW** #10(a) for definition.
[12] Civ. Code § 1798.140(ae). See **EXISTING LAW** #10(b) for definition.
[13] A comparison chart of state privacy laws can be accessed at https://45555314.fs1.hubspotusercontent-na1.net/hubfs/45555314/Slides%20and%20one-pagers/US%20state%20law%20comparison%20chart_2024_July_1.pdf.

One could argue that the State's current consumer privacy laws fall short of the protections envisioned by the Legislature and the voters in 1972. The proponents argued for a much more stringent level of protection – the right to be left alone. The authors of the proposition promised that adding a right to privacy would ensure the protection of "our homes, our families, thoughts, our emotions, our expressions, our personalities, our freedom of communion, and our freedom to associate with the people we choose."[14] In 2025, a person would be hard-pressed to find that level of privacy in their homes, much less outside of those formerly private spheres.

5) **Governor's veto of AB 3048 (Lowenthal, 2024).** This bill is essentially identical to a bill proposed by the author last year that was vetoed by the Governor. In his veto message, the Governor noted:

> I am 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.

However, in arguing for the ease of adding an opt-out signal for operating systems and search engines, Consumer Reports argues in their support letter:

> 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.

While not an opt-out signal in terms of sharing and selling personal information, Apple's universal opt-out feature, which was added to their operating system a several years ago, allows users to universally opt out of giving app developers permission to track the users' activities across other applications. This means any app that tries to ask for a user's permission will be automatically blocked from asking to track the user and informed of the user's preference to opt out of tracking. Thus, supporters contend that the essential design question has, in effect, been addressed by at least one major developer.

In response to the Governor's veto, the Privacy Agency notes:

> Consistent with the Governor's comments, AB 566 would leave room for stakeholders, including developers, to help determine the best methods of recognizing and implementing the opt-out preference signals. Using an opt-out preference signal is the single most important step a California consumer can take to protect their privacy. In light of significant changes on the federal level, it is more important than ever that Californians are able to protect their privacy.
>
> While it is true that no major mobile OS incorporates an option for an opt-out signal, requiring mobile operating systems to offer opt-out preference signals would enable consumers to stop the sale and sharing of their personal information by all apps in a single

---

[14] *Right of Privacy California Proposition 11*, UC L. SF SCHOLARSHIP REPOSITORY (1972), pp. 26–27, https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props..

step. Thus, it protects the primary way consumers, including many children, use the internet – through apps on their phones. Clearly, existing protections are not enough. Apps commonly share personal information with ad networks on Android devices, and a number of apps have claimed that they can circumvent Apple's privacy features - including Shopify and Google, Meta, and Spotify.

Through this bill, we seek to continue to work with stakeholders, learn how they might envision such a tool, and identify the best path forward. In addition, the CPPA is committed to working with stakeholders to develop regulatory specifications that work with their systems before a mobile requirement would go into effect.

6) **What this bill would do.** As noted above, in order for a consumer to exercise their privacy rights, they must affirmatively opt out of the sharing and selling of their personal information on every website and with virtually every business they interact with. Currently, in order to take advantage of a universal opt-out preference signal to submit opt-out requests under California law, consumers must either use one of the few browsers that support an opt-out preference signal or take additional steps to locate and download a third-party browser plugin that adds support for such signals.

This bill, would require that all search platforms and mobile operating systems develop a universal opt-out preference signal for users. This universal opt-out allows a consumer to toggle a switch on their internet browser or in their mobile device settings that sends a signal on behalf of the consumer communicating their decision to opt out of the sale and sharing of their personal information. Thus allowing users to communicate privacy preferences to the host of the websites rather than having to manually indicate the user's preferences on each website the user visits. Upon receiving this signal, websites cannot sell or share the consumer's personal information absent some affirmative action from the consumer granting permission to the respective website.

7) **Amendments.** The author has agreed to make two amendments. The first would delete the language authorizing the Privacy Agency to change the statutory definitions of "browser" and "mobile operating system" through their regulatory process. Specifically, the amendment does the following:

(c) The California Privacy Protection Agency may adopt regulations as necessary to implement and administer this section~~, including, but not limited to, ensuring that the setting described by subdivision (a) is easy for a reasonable person to locate and configure. and updating the definitions of "browser" and "mobile operating system" to address changes in technology, data collection, obstacles to implementation, or privacy concerns~~.

Second, opposition notes that the bill in print contains the confusing construction, "[u]nless otherwise prohibited by federal law, a business shall not …" Because preemption does not appear to be a clear concern and, in any event, would apply regardless of whether this bill acknowledges federal law, the author has agreed to the following technical amendment to remove the language in the bill:

(a) (1) ~~Unless otherwise prohibited by federal law, a~~ ***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.

ARGUMENTS IN SUPPORT: The California Privacy Protection Agency, sponsors of the bill, write in support:

> Opt-out preference signals like the Global Privacy Control (GPC) are important innovations as they significantly simplify consumers' ability to exercise their rights to opt-out of sale under the CCPA by enabling them, in a single step, to send an opt-out request to every site with which they interact online. The California Consumer Privacy Act of 2018 (CCPA) currently requires businesses to honor opt-out preference signals as a request to opt-out of the sale of their personal information. The California Department of Justice included this in their CCPA regulations, adopted in 2020, and the CPPA's regulations, adopted in 2023, update the opt-out preference signal requirement.
>
> However, only a handful of browsers currently offer native support for opt-out preference signals. Google Chrome, Microsoft Edge, and Apple Safari—which make up over 90% of the desktop browser market share—have declined to offer these signals. Importantly, none are loaded onto devices by default.
>
> The lack of signal uptake by browsers has created a burden for consumers. Today, to take advantage of their right to use an opt-out preference signal to submit opt-out requests under California law, consumers must either find one of the few privacy-focused browsers or take extra steps to locate and download a browser plugin created by third-party developers that adds support for such signals, which can introduce additional privacy and security concerns. Further, consumers accessing the internet through an Apple mobile device have no access to these signals.

ARGUMENTS IN OPPOSITION: In opposition to the bill, the California Chamber of Commerce, along with a number of other business organizations, raises a number of concerns about the bill. They argue:

> 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. . . to adopt regulations around that voluntary use.
>
> [. . .]
>
> 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.
>
> [. . .]
>
> 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.

REGISTERED SUPPORT / OPPOSITION:

Support

California Privacy Protection Agency (Sponsor)
Brave Software
Center for Democracy and Technology
Center for Digital Democracy
Center for Economic Justice
Check My Ads
Common Sense Media
Concept Art Association
Consumer Action
Consumer Attorneys of California
Consumer Federation of America
Consumer Reports
Consumer Watchdog
Digital Content Next
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Los Angeles County Democratic Party
Mozilla
Oakland Privacy
Privacy Researchers and Academics
Privacy Rights Clearinghouse
Santa Monica Democratic Club
Secure Justice
Virginia Citizens Consumer Council

Opposition

American Advertising Federation (AAF)
American Association of Advertising Agencies (4A's)
Association of National Advertisers
California Chamber of Commerce
California Retailers Association
Chamber of Progress
Computer and Communications Industry Association
Connected Commerce Council
Digital Advertising Alliance
Insights Association
Interactive Advertising Bureau
Software Information Industry Association
Technet
Valley Industry and Commerce Association (VICA)

Oppose Unless Amended

Calbroadband
Network Advertising Initiative

Analysis Prepared by: Julie Salley / P. & C.P. / (916) 319-2200