Date of Hearing: April 2, 2024

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 3048 (Lowenthal) – As Introduced February 16, 2024

AS PROPOSED TO BE AMENDED

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

SYNOPSIS

Some people consider sharing their personal information, including the websites they visit, purchases they make, employment history, menstrual cycles, name, phone number, address, pictures, locations and movements, social media posts and reactions, and other seemingly innocuous information when taken individually, a reasonable price to pay for freely accessing the internet. However, not protecting that personal information can have real world consequences when it comes to searching for a job, purchasing a house, obtaining credit, opening a bank account, interacting with law enforcement, or trying to escape a dangerous and violent intimate partner.

As a way of giving Californians more power over how and when their personal information is collected, used, shared, and sold, the California Consumer Privacy Act (CCPA) grants us the right to direct a business to not sell or share our personal information at any time. However, despite the rights enshrined in the law, exercising those rights remains challenging, even for the most conscientious individuals.

This bill, sponsored by the California Privacy Protection Agency (Privacy Agency), endeavors to make it significantly easier for consumers to opt out of the sharing or sale of their personal information by requiring internet browsers to provide an opt-out preference signal that they can use to signal all of the businesses they interact with online that they are exercising their rights under the CCPA by prohibiting the businesses from sharing their personal information.

As Oakland Privacy notes in their support of this bill, "A right that is difficult to exercise becomes a conditional right: i.e. one that is only available if you are determined enough and computer-savvy enough to be able to utilize it. But the intention of the California Privacy Rights Act was not a conditional right to control the sale and sharing of your personal information. It was intended, and sold to voters, as an absolute right."

Along with the Privacy Agency and Oakland Privacy, this bill is supported by Secure Justice and the Electronic Frontier Foundation (with the committee amendments). It is opposed by a coalition of business groups, including the Association of National Advertisers, California Chamber of Commerce, California Land Title Association, and California Retailers Association.

SUMMARY: Requires that internet browsers 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. Specifically, **this bill**:

1) Prohibits a business from developing or maintaining a browser 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 be relatively easy for consumers to locate and enable.

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

4) Allows the California Privacy Protection Agency (Privacy Agency) to adopt regulations to implement and administer this legislation, including updating the definitions of "browser" and "device" 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 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.

10) Defines the following terms under the CCPA:

a) "Business" means a for-profit entity that collects consumers' personal information, does business in California, and meets one or more of the following criteria:

i) It had gross annual revenue of over $25 million in the previous calendar year.

ii) It buys, receives, or sells the personal information of 100,000 or more California residents, households, or devices annually.

iii) It derives 50% or more of its annual revenue from selling California residents' personal information. (Civ. Code § 1798.140(d).)

b) "Consumer" means a natural person who is a California resident. (Civ. Code § 1798.140(i).)

c) "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).)

d) "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).)

FISCAL EFFECT: As currently in print, this bill is keyed fiscal.

COMMENTS:

1) **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.[1]

Since the time this piece was published, it has become increasingly clear that not only is 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 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.[2]

---

[1] Preston, Alex. "The death of privacy." *The Guardian* (Aug. 3, 2014) *available at* https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston.
[2] Zuboff, Shoshana. "You Are the Object of a Secret Extraction Operation." *The New York Times* (Nov. 12, 2021) *available at* https://www.nytimes.com/2021/11/12/opinion/facebook-privacy.html.

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, not protecting that personal 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.[3] 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.[4]

As noted above, the slow erosion of privacy, through the collection of 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."[5]

Catherine Powell pointed out in 2023 in a blog post for the *Council on Foreign Affairs*:

> 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 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.[6]

2) **Purpose of this bill.** This bill, sponsored by the Privacy Agency, is intended to make it easier for consumers to limit the amount of personal information being collected every time they search for anything on the internet. In his letter of support, the executive director of the Privacy Agency, Ashkan Soltani, states, "Opt-out preference signals such as the Global Privacy Control (GPC) are important innovations as they significantly simplify consumers' ability to exercise their rights to

---

[3] Hern, Alex. "Grindr fined £8.6m in Norway over sharing personal information," *The Guardian* (Jan. 26, 2021) *available at* https://www.theguardian.com/technology/2021/jan/26/grindr-fined-norway-sharing-personal-information.
[4] "Grindr shared information about users' HIV status with third parties." *The Guardian* (Apr. 3, 2018) *available at* https://www.theguardian.com/technology/2018/apr/03/grindr-shared-information-about-users-hiv-status-with-third-parties.
[5] Clarke, Laurie. "Interview - Law professor Danielle Citron: 'Privacy is essential to human flourishing,'" *The Guardian* (Oct. 2, 2022) *available at* https://www.theguardian.com/technology/2022/oct/02/danielle-citron-privacy-is-essential-to-human-flourishing.
[6] Powell, Catherine. "Data is the New Gold, But May Threaten Democracy and Dignity," *Council on Foreign Relations* (Jan. 5, 2023) *available at* https://www.cfr.org/blog/data-new-gold-may-threaten-democracy-and-dignity-0.

opt-out of sale under the CCPA by enabling them to send an opt-out request to every site with which they interact online, without having to make separate requests at each business."

According to the author, in order to take advantage of their right to use an opt-out preference signal to submit opt-out requests under California law, currently 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. As of the writing of this analysis, only Mozilla Firefox, DuckDuckGo, and Brave offer support for opt-out preference signals, which, together, make up less than 10% of the overall global desktop browser market share.

The operators of the world's largest internet browsers, most notably, Alphabet who owns Chrome, Apple that runs Safari, and Microsoft that operates Edge, have declined to adopt an opt-out preference signal to allow users of their browser to indicate they do not want their personal information sold or shared by any URL they visit while using the browser. These companies make up over 90% of the desktop browser market and also rely on advertising business models for their revenue, perhaps making it unlikely that they will voluntarily create an opt-out signal on their browsers. Because of this reality, the purpose this bill is to require all businesses with internet browsers used by the general public to develop an opt-out preference signal that consumers can easily find and use to opt-out of having their information collected by the websites they visit.

3) **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, but many of the top web browsers do not offer such signals. AB 3048 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.

4) **What is an opt-out preference signal?** An opt-out preference signal, such as Global Privacy Controls (GPC), are a signal that is sent by a third-party platform on behalf of the consumer that communicates the consumer's choice to opt out of the sale and sharing of their personal information. Essentially, these signals are a way for users to communicate privacy preferences to a host of websites by using a specific search engine or browser plug-in 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.

5) **The California Consumer Privacy Act and the California Privacy Rights Act (CPRA).** In 2018, the Legislature enacted the CCPA (AB 375 (Chau, Chap. 55, Stats. 2018)), which gives consumers certain rights regarding their personal information, such as the right to: (1) know what personal information about them is collected and sold; (2) request the categories and specific pieces of personal information the business collects about them; 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. With the passage of the CCPA and the CPRA, California now has the most comprehensive laws in the country when it comes to protecting consumers' rights to privacy.

In addition, Proposition 24 created the Privacy Agency in California, vested with full administrative power, authority, and jurisdiction to implement and enforce the CCPA and the CPRA. The Agency's responsibilities include updating existing regulations, and adopting new regulations.

To protect Californians from any future legislative efforts to weaken statutory protections in the CPRA, Proposition 24 provided that the CPRA's contents may be amended by a majority vote of the Legislature only if the amendments are consistent with and further the purpose and intent of the CPRA, which is to further protect consumers' rights, including the constitutional right of privacy.[7]

6) **Analysis.** As discussed previously, the amount of personal, intimate information that is being collected and compiled into dossiers online is not necessarily harmless nor does it have to be the price users pay to be able navigate the internet. California has been on the forefront of developing robust privacy protection laws, especially the CCPA. However, over the last year or two, policymakers have been dealing with the fact that despite the rights enumerated in the CCPA, exercising those rights remains nearly impossible. Currently, the burden of exercising privacy rights is placed completely on individuals, requiring them to seek out each company that has collected their data and figure out how to request that they delete it or stop collecting it.

The CPRA contemplated the need for an opt-out signal and requires the Privacy Agency to promulgate regulations defining the requirements and technical specifications for two opt-out signals, a general opt-out for consumers, and one that can be used to allow children and their parents to indicate that they are under 16 and therefore afforded extra protections [see **EXISITNG LAW** #9]. Unfortunately the CPRA was less clear about requiring businesses subject to privacy laws to adopt an opt-out signal or any other single tool that makes it easy for consumers to exercise their rights.

Oakland Privacy, writing in support of the bill, explains:

> The current version of the CPRA contains an overly complicated set of alternative options that, while they apparently seemed desirable during the drafting phase, have not made opting out easy or simple for users. Anyone browsing the Internet nowadays is aware of the endless series of opt-out windows presented in varying styles, formats and places by virtually every website they visit. It is a rare internet user who does not mumble in exasperation that they wish they could just check it once and have it apply to all websites.

Instead of requiring a single method for allowing consumers to exercise their privacy rights, the CPRA required businesses to offer specific links on their websites that allow consumers to opt-out, unless they choose to honor the information provided by an opt-out preference signal [see **EXISITNG LAW** #7 and 8]. The author and supporters argue that the CPRA's failure to require a standardized opt-out process has made it difficult to reach the law's full intent, which is to further Californians' right to protect their privacy.

The opponents of the bill, a coalition of businesses, argue that requiring an opt-out preference signal is contrary to the CPRA, which intentionally allows businesses to implement the most effective method for their business. They state, "[The bill] will upend the balanced approach

---

[7] Ballot Pamphlet. Primary Elec. (Nov. 3, 2020) text of Prop. 24, p. 74

taken by voters, removing any such flexibility in the law." Arguably, however, while this bill requires browsers to include an easy to locate opt-out preference signal, it does not prohibit individual websites from continuing to offer individual links that allow consumers to opt-out. Having both of these options available allows those consumers who would like to exercise a universal opt-out to do so, while allowing others to be selective in terms of which companies they allow to sell, share, and use their personal information and sensitive personal information.

Aside from requiring browsers to adopt an opt-out preference signal, the opponents argue that the language in the bill is not clear. They write:

> As drafted, it is unclear whether the business has to refrain from developing or maintaining a browser that does not include a setting that enables a consumer to send an opt-out preference signal to other businesses that the consumer interacts with *or* the business that develops or maintains the browser has to somehow prevent the consumer from interacting with another business that fails to include a setting that allows them to send a signal to the other business.

As currently written, the bill states:

> (a) (1) A business shall not develop or maintain a browser through which a consumer interacts with a business that does not include a setting that enables the consumer to send an opt-out preference signal to that business.

The opposition makes a valid point. As written, the requirement on businesses could be misconstrued. Committee amendments are intended to eliminate this confusion.

The proponents of the CPRA clearly stated that the act was intended to give consumers the power to stop businesses from tracking them without their knowledge and permission.[8] Overall, requiring browsers to offer opt-out preference signals would significantly increase consumers' ability to avail themselves of this right by sending a signal to every website they interact with that they are exercising their right to opt-out of the sale and sharing of their personal information.

7) **Proposed Committee amendments.** In order to address the concerns raised by the opposition and the Electronic Frontier Foundation related to sections of the bill that were unclear, the Committee amendments do the following:

Amendment #1 clarifies the requirements being placed on businesses.

> 1798.136(a) (1) A business shall not develop or maintain a browser ~~through which a consumer interacts with a business~~ that does not include a setting that enables ~~the~~ consumer***s*** to send an opt-out preference signal to ~~that~~ ***other*** business***es that the consumer interacts with through the browser***.

Amendment #2 recognizes the many different forms a browser may take. For example, on smaller devices it may not be "easy to locate and use" any settings. The change in the language allows for the differences in devices

> 1798.136 (a)(2) The setting required by paragraph (1) shall be ***reasonably*** easy to locate and ***enable*** ~~use~~.

---

[8] Ballot Pamphlet. Primary Elec. (Nov. 3, 2020) text of Prop. 24, p. 70

Amendment #3 is intended to narrow and clarify the definition of "browser."

> 1798.136 (d) As used in this section, "browser" means a***n interactive*** software application ***that is primarily used by a consumer to*** ~~for~~ access~~ing internet~~ websites ~~and information~~ ***on the internet***.

8) **Related legislation.** Over the last 5 years numerous bills have attempted to modify the CCPA and many have been successful in furthering its goals. In this hearing, alone, three bills, including this one, propose modifications to the CCPA. Specifically:

AB 1824 (Valencia) requires, under the CCPA, that businesses that are acquiring the personal data of consumers through the acquisition of another business, honor the previous decisions of consumers who have not given permission for the business to sell or share their personal information.

AB 1949 (Wicks) proposes amending the CCPA to prohibit a business from collecting the personal information of a consumer under 18 years of age unless the consumer, or the consumer's parent or guardian if under 13, affirmatively authorizes the collection.

REGISTERED SUPPORT / OPPOSITION:

Support

California Privacy Protection Agency
Oakland Privacy
Secure Justice

Support If Amended

Electronic Frontier Foundation

Opposition

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

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