CONCURRENCE IN SENATE AMENDMENTS
AB 566 (Lowenthal)
As Amended September 5, 2025
Majority vote

SUMMARY

This bill 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.

Senate Amendments
1) Deletes browser engines.

2) Deletes requirement that a business that develops and maintains a browser disclose the types of personal information to which the opt-out preference signal would apply.

3) Declares that a business that includes a functionality that enables the browser to send an opt-out preference signal is not liable for a violation of this title by a business that receives the signal.

4) Delays implementation until January 1, 2027.

COMMENTS

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 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:

---

[1] 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.

> 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]

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."[3]

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.[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.[5] 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. . . ."[6]

---

[2] 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.
[3] 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.
[4] 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.
[5] California Proposition 11 (1972), "Constitutional Right to Privacy Amendment."
[6] *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.

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,[7] 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.[8] 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.[9] 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.

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. >

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

---

[7] Civ. Code Section 1798.140(v). See *EXISTING LAW* no. 10(a) for definition.
[8] Civ. Code Section 1798.140(ae). See *EXISTING LAW* no. 10(b) for definition.
[9] 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

.

> 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.
>
> [. . .]
>
> 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, argues:

> 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.

FISCAL COMMENTS

Minor and absorbable costs to the California Privacy Protection Agency (Privacy Agency) to issue regulations and enforce the opt-out preference signal requirement. The Privacy Agency anticipates initial costs will be absorbable but its Legal Division may seek additional resources if recurring rulemaking is necessary in the future.

VOTES:

ASM PRIVACY AND CONSUMER PROTECTION: 9-0-6
YES: Berman, Bryan, Irwin, Lowenthal, McKinnor, Ortega, Pellerin, Ward, Wilson
ABS, ABST OR NV: Bauer-Kahan, Dixon, DeMaio, Macedo, Patterson, Petrie-Norris

ASM APPROPRIATIONS: 11-0-4
YES: Wicks, Arambula, Calderon, Caloza, Elhawary, Fong, Mark González, Hart, Pacheco, Pellerin, Solache
ABS, ABST OR NV: Sanchez, Dixon, Ta, Tangipa

ASSEMBLY FLOOR: 53-1-25
YES: Addis, Aguiar-Curry, Ahrens, Alvarez, Arambula, Ávila Farías, Bauer-Kahan, Bennett, Berman, Boerner, Bonta, Bryan, Calderon, Caloza, Carrillo, Connolly, Elhawary, Fong, Gabriel, Garcia, Gipson, Mark González, Haney, Harabedian, Hart, Jackson, Kalra, Krell, Lee, Lowenthal, McKinnor, Muratsuchi, Nguyen, Pacheco, Pellerin, Quirk-Silva, Ramos, Ransom, Celeste Rodriguez, Rogers, Blanca Rubio, Schiavo, Schultz, Sharp-Collins, Solache, Soria, Stefani, Valencia, Ward, Wicks, Wilson, Zbur, Rivas

NO: DeMaio
ABS, ABST OR NV: Alanis, Bains, Castillo, Chen, Davies, Dixon, Ellis, Flora, Gallagher, Jeff Gonzalez, Hadwick, Hoover, Irwin, Lackey, Macedo, Ortega, Papan, Patel, Patterson, Petrie-Norris, Michelle Rodriguez, Sanchez, Ta, Tangipa, Wallis

UPDATED

VERSION: September 5, 2025

CONSULTANT: Julie Salley / P. & C.P. / (916) 319-2200 FN: 0001997