Date of Hearing: April 21, 2026
Fiscal: No

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 2561 (Valencia) – As Introduced February 20, 2026

PROPOSED AMENDMENTS

SUBJECT: Operating systems and applications: privacy settings

SYNOPSIS

Despite State laws providing consumer protections and enshrining the right to privacy for all individuals, websites, applications, and operating systems continue to collect mass amounts of personal information from users, often without user awareness or consent. This data is then sold to data brokers, who can market this data to anyone interested in purchasing it.

This bill aims to increase privacy protections for consumers by requiring that operating systems and applications set a user's default privacy setting as the most protective setting offered by the operating system or application. In addition, this bill prohibits an operating system or application from changing a user's privacy settings without consent from the user.

Proposed Committee amendments, outlined in Comment #4, restrict the bill to prohibiting operating systems or applications from undoing a user's privacy settings without user consent and adds a cross-reference to a standing definition of consent.

This bill is author-sponsored. It is supported by Oakland Privacy and the Consumer Federation of California. Although the bill in print has opposition, their concerns relate solely to provisions that will be omitted via the Committee amendments; consequently, the bill, as proposed to be amended, has no registered opposition.

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) Requires social media platforms to provide a clear and conspicuous button to delete their account and provide the user with the necessary steps to delete the user's account and information. (Civ. Code § 3273.90.)

5) Establishes the Data Broker Registration, housed under the California Consumer Privacy Agency, to register data brokers and provide a one-click mechanism for consumers to request that registered data brokers delete their personal information (Civ. Code §§ 1798.99.80-1798.99.89.)

THIS BILL:

1) Defines "application" as a software program, mobile app, or desktop app that collects, processes, or stores personal information about a user in the state and that provides privacy settings allowing the user to control the collection, use, sharing, or disclosure of that personal information.

2) Defines "privacy setting" as any user-configurable option within an application that governs the application's collection, use, sharing, disclosure, retention, or processing of the user's personal information.

3) Requires an operating system or an application to configure a user's default privacy setting to be the most privacy protective setting offered by the operating system or application.

4) Prohibits an operating system or an application from changing a user's privacy setting without the user's explicit consent.

COMMENTS:

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

> AB 2561 strengthens privacy protections for consumers by ensuring that software companies and applications do not change privacy settings without their explicit consent. The overwhelming majority of Californians strongly desire data minimization. However, the default settings for many software systems and apps are the least privacy protected and are designed to have the user share their data, often times for profit and without their knowledge. Further, it is not uncommon after a software or app update, for user's privacy settings to be changed. If a user is savvy enough to notice a difference in their settings, the onus falls on them to troubleshoot the issue and re-adjust their privacy setting to what it was prior to the update. AB 2561 would prioritize user's privacy rights and ensure they remain in control of their data.

2) **Background.** The operating system (commonly called OS) on a person's phone, tablet, or computer is the interface between the device's software and hardware. The operating system allows applications to access the internet, access the computer's hard-drive, and to generally

operate as intended.[1] These systems therefore have access to everything that a person has viewed or engaged with on the device, and can pass that information "upstream," "for a variety of reasons, ranging from beneficial and benign (such as information used to make the software better) to malicious and invasive (such as truly tracking what you as an individual are doing)".[2]

Access to such vast quantities of personal data collected from applications and operating software has led to a burgeoning market, coined by social psychology Shoshana Zuboff as "surveillance capitalism."[3] According to Zuboff, surveillance capitalism is an economic system built on the secret extraction and manipulation of human data.[4] Knowing what an individual views online, the purchases they make from online retail stores, and even how they communicate with friends and family over instant messaging apps can be a marketing gold-mine for advertisers, who have long attempted to understand the probability that an individual would engage with, or be persuaded by, an advertisement. By developing complex computer algorithms that would sort through collected user information and infer certain traits – searches for "symptoms of prostate cancer", for instance, may lead to inferences that the user is over 45-years old and male – early pioneers of surveillance capitalism such as Google revolutionized advertising through ubiquitous online surveillance.[5]

Surveillance capitalism has led to the growth of data brokers, who purchase the personal data collected by Google and other applications and sell it to whomever is willing to pay for the information. Currently, there are over 4,000 data brokers with dossiers on 98% of the people in the United States.[6] The largest data broker, Acxiom, has more than 10,000 data attributes on over 2.5 billion people in more than 60 countries.[7] To attempt to protect the troves of data shared amongst applications and operating systems, the CCPA requires any for-profit entity doing business in California that collects or processes consumers' personal information to provide a CCPA privacy policy if the company meets any of the following requirements:

1. Has annual gross revenues in excess of $25 million.

2. Either alone, or in combination, buys, receives for commercial purposes, sells, or shares for commercial purposes the personal information of 100,000 or more consumers, households, or devices.

3. Derives half or more of its annual revenue from selling a consumer's personal data.[8]

Personal information includes any information that identifies, is related to, or could be linked to a specific individual or their household, directly or indirectly. This includes names or nicknames, email addresses, purchase history, browsing history, location data, employment data, IP

---

[1] Leo A. Notenboom, "Privacy Begins with the Operating System," *Ask Leo!* (July 10, 2023), https://askleo.com/privacy-begins-operating-system/.
[2] *Id.*
[3] Zuboff, Shoshana, "You are the Object of a Secret Extraction Operation," *New York Times* (Nov. 12, 2021). https://www.nytimes.com/2021/11/12/opinion/facebook-privacy.html.
[4] *Id.*
[5] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* 1st ed. (New York: Public Affair, 2018), p. 78-79.
[6] Solove, Daniel J. Privacy in Authoritarian Times: Surveillance Capitalism and Government Surveillance, George Washington University Law School (Jan. 19, 2025). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5103271.
[7] *Id.*
[8] Civ. Code § 1798.140 (d).

addresses, profiles created by businesses about an individual, and sensitive personal information such as social security number, genetic data, financial account or credential information, race or ethnic origin, citizenship, biometrics such as facial recognition patterns, and information pertaining to a person's health, sex life, or sexual orientation.[9]

3) **What the bill, as proposed to be amended, would do.** The growth of data brokers and the economy of personal information have led to increased privacy concerns. This bill, in its proposed to be amended form, would require that operating systems and applications receive a user's consent prior to undoing any user privacy settings.

Given the rise of data brokers, consumers are becoming more cognizant of the risk of sharing mass amounts of data with every website, app, or device that they use. According to Oakland Privacy, supporters of the bill:

> Polling data supports that the majority of the population wants to, and would, use the privacy settings on their browsers and operating systems and applications to limit sales, shares and repurposing of their data to the extent that they can do so.[10]

Privacy settings allow for, at least in theory, user control over the tracking and sharing of their personal data. However, recent news reports suggest that applications and websites may not be respecting user choice. An independent audit of Microsoft, Google and Meta web traffic in California found that 55 percent of the investigated sites set advertising cookies in a user's browsers despite the user opting out of tracking.[11] Additionally, application software and operating systems may re-enable certain privacy options that users had switched off following system updates, as Apple iOS 17 did in 2023.[12] Following the iOS 17 update, a few privacy-savvy users noticed that two privacy settings that they had previously toggled off – "Significant Locations" and "iPhone Analytics" – were turned back on. While "Significant Locations" remains local to a user's iPhone and is not accessible by Apple, "iPhone Analytics" is used by Apple to collect "details about hardware and operating system specifications, performance statistics, and data about how you use your devices and applications. This information is used to help Apple improve and develop its products and services."[13] Oakland Privacy writes:

> AB 2561 addresses what [we] would call privacy-slamming. It is not uncommon for software of applications to perform "quiet updates" where a user's privacy settings, data collection, and tracking are re-set to the maximum data collection default without their explicit consent. If a user is savvy enough to recognize changes to their settings, they must manually troubleshoot their issue and re-adjust to their settings to what they were before the update. This re-adjustment has become increasingly layered and complex to navigate.

---

[9] "What is personal information?" *privacy.ca.gov, https://privacy.ca.gov/protect-your-personal-information/what-is-personal-information/* .
[10] https://yougov.com/en-us/articles/53862-data-privacy-day-us-2026-how-concerned-are-americans-about-data-security.
[11] Matthew Gault, "Google, Microsoft, Meta All Tracking You Even When You Opt Out, According to an Independent Audit," *404 Media,* (Apr. 14, 2026), https://www.404media.co/google-microsoft-meta-all-tracking-you-even-when-you-opt-out-according-to-an-independent-audit/?ref=daily-stories-newsletter.
[12] Graham Cluley, "iOS 17 update secretly changes your privacy settings; here's how to set them back," *Bitbender,* (Sept. 25, 2023), https://www.bitdefender.com/en-au/blog/hotforsecurity/ios-17-update-secretly-changed-your-privacy-settings-heres-how-to-set-them-back.
[13] *Id.*

> By preventing the privacy protections a user has in place from being changed without their explicit consent, AB 2561 is a user protection bill that removes a dark pattern process that frustrates the intentions of the user and increases the friction in maintaining and using available privacy controls on web browsers and applications. We are all too busy and distracted to be assigned an ongoing burden of regularly checking the privacy settings on our browsers and all the applications we use to check that they have not been slammed back to a maximum collection default when we weren't looking.

4) **Amendments.** To address opposition's concerns about the feasibility and operational impacts of establishing a "most privacy protective" setting, the author has agreed to the following amendments. The first amendment strips the requirement for operating systems to have the most privacy protective setting by default. The second amendment adds a definition of consent from the CCPA. Technical amendments add clarity to the requirement that operating systems and applications do not change a user's privacy settings without consent. The bill, in its entirety, will read as follows:

> 22683**.** As used in this chapter:
>
> (a) "Application" means a software program, mobile app, or desktop app that collects, processes, or stores personal information about a user in the state and that provides privacy settings allowing the user to control the collection, use, sharing, or disclosure of that personal information.
>
> ***(b) "Consent" has the same meaning defined in Section 1798.140 of the Civil Code.***
>
> (c~~b~~) "Personal information" has the meaning defined in Section 1798.140 of the Civil Code.
>
> (d~~c~~) "Privacy setting" means any user-configurable option within an ***application's privacy settings menu or similarly labeled menu*** that governs the application's collection, use, sharing, disclosure, retention, or processing of the user's personal information.
>
> 22684**.** ~~(a) An operating system or an application shall configure a user's default settings to be the most privacy protective setting offered by the operating system or application.~~
>
> ~~(b)~~ An operating system or an application shall not *undo* change a user's ***affirmative configuration of a*** privacy setting without the user's ~~explicit~~ consent.

ARGUMENTS IN SUPPORT: Consumer Federation of California, supporters of the bill, write:

> Earlier this year, *The New York Times* reported that tech companies are increasingly updating their systems by incorporating AI tools into social media, email, and search engine platforms, often automatically opting consumer in without their consent in order to get around privacy laws that restrict the tracking of people's activity.[14] Once consumers have been opted in, it is extremely difficult, if not, impossible to opt-out and turn off unwanted tools that collect consumer's information. These practices are only growing and for these reasons, we believe that AB 2561 is a step in the right direction. Through this bill, we can help ensure that

[14] Brian Chen (2026), "A.I is giving you a personalized internet, but you have no say in it," The New York Times, https://www.nytimes.com/2026/02/10/technology/personaltech/ai-google-meta-opt-out.html.

updates to operating systems and applications do not come at the expense of a consumer's privacy and choice.

REGISTERED SUPPORT / OPPOSITION:

Support

Consumer Federation of California
Oakland Privacy

Opposition

California Chamber of Commerce
Computer and Communications Industry Association
Los Angeles County Moms for Liberty
TechNet

Analysis Prepared by: Kate Davis / P. & C.P. / (916) 319-2200