

SENATE PRIVACY, DIGITAL TECHNOLOGIES, AND CONSUMER PROTECTION COMMITTEE
Senator Christopher Cabaldon, Chair
2025-2026 Regular Session

AB 2561 (Valencia)
Version: April 23, 2026
Hearing Date: June 8, 2026
Fiscal: No
Urgency: No
CK

SUBJECT

Operating systems and applications: privacy settings

DIGEST

This bill prohibits an operating system or application from undoing a user's affirmative configuration of a privacy setting without the user's consent.

EXECUTIVE SUMMARY

Consumer data collection has become an inescapable feature of modern digital life, with operating systems, applications, and online services continuously gathering information about your location, browsing habits, purchase history, device usage, and even physical activity. This is often done in ways that are not immediately visible to the average user. Tech companies, advertisers, and data brokers aggregate this information to build detailed profiles that can influence everything from the ads a consumer sees to the prices they are offered, and in some cases, the data is sold to or accessed by third parties the consumer never interacted with.

Privacy settings on operating systems such as Windows, macOS, iOS, and Android allow users to review and set permissions granted to apps, limit location tracking, disable telemetry and diagnostic sharing, and restrict ad personalization. At the app level, consumers generally have the ability to control access to their camera, microphone, contacts, and storage, and to opt out of data sharing features.

This bill ensures that those consumers who take advantage of these options and configure their privacy settings are having their preferences honored. The bill prohibits an operating system or application from undoing a user's affirmative configuration of a privacy setting without the user's consent.

The bill is author sponsored. No timely support or opposition has been received by this Committee.

PROPOSED CHANGES TO THE LAW

Existing law:

- 1) Provides, pursuant to the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const., art. I, § 1.)
- 2) Establishes the California Consumer Privacy Act (CCPA), which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. It places attendant obligations on businesses to respect those rights. It does not apply to government entities. (Civ. Code § 1798.100 et seq.)
- 3) Defines “personal information” for purposes of the CCPA as 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. The CCPA provides a nonexclusive series of categories of information deemed to be personal information, including biometric information, geolocation data, and “sensitive personal information.” (Civ. Code § 1798.140(v)(1).)
- 4) Defines “consent” for purposes of the CCPA as any freely given, specific, informed, and unambiguous indication of the consumer’s wishes by which the consumer, or the consumer’s legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent. (Civ. Code § 1798.140(h).)

This bill:

- 1) Prohibits an operating system or an application from undoing a user’s affirmative configuration of a privacy setting without the user’s consent.
- 2) Defines the relevant terms:
 - 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” and “personal information” have the same meaning as laid out in the CCPA.
- c) “Privacy setting” means any user-configurable option within an application’s privacy, or similarly labeled, menu that governs the application’s collection, use, sharing, disclosure, retention, or processing of the user’s personal information.

COMMENTS

1. The collection and commodification of consumer data

The Federal Trade Commission (FTC) has highlighted the breadth of this new era of widespread data collection, especially through consumers’ smartphones:

For many of us, our mobile phone is a constant companion, with us wherever we go. It’s also constantly collecting information about us, what we do, and where we do it. And unbeknownst to many of us, once that information is collected, much of it gets sold onwards in a murky marketplace of data brokers and advertisers. Because this market for our data is not transparent, it’s almost impossible to figure out who has information about us and what they’re doing with it.

Our phones can also reveal far more about us than we might realize: important details about our lives and where we’ve been. For example, our phones might be periodically sending their exact location to tech companies. This data can pinpoint our comings and goings with startling precision. Think what this might reveal: what therapist you’re seeing, what medical treatment you’re seeking, your visits to places of worship, and even your reproductive choices. This type of tracking can cause enormous harm to consumers, including stigma, emotional distress, discrimination, or even physical violence.¹

The commodification of this personal information has been dubbed “surveillance capitalism” by social psychologist, Shoshana Zuboff:

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

¹ Carol Kando-Pineda. *Consumer Alert: FTC sues company that sells consumers’ sensitive location information* (August 29, 2022) FTC, <https://consumer.ftc.gov/consumer-alerts/2022/08/ftc-sues-company-sells-consumers-sensitive-location-information>. All internet citations are current as of June 1, 2026.

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

Consumers’ information can even be used to charge them more for products and services, a practice known as surveillance pricing. Again, according to an FTC study:

The staff perspective is based on an examination of documents obtained by FTC staff’s 6(b) orders sent to several companies in July aiming to better understand the shadowy market that third-party intermediaries use to set individualized prices for products and services based on consumers’ characteristics and behaviors, like location, demographics, browsing patterns and shopping history.

Staff found that consumer behaviors ranging from mouse movements on a webpage to the type of products that consumers leave unpurchased in an online shopping cart can be tracked and used by retailers to tailor consumer pricing.

“Initial staff findings show that retailers frequently use people’s personal information to set targeted, tailored prices for goods and services – from a person’s location and demographics, down to their mouse movements on a webpage,” said FTC Chair Lina M. Khan.³

2. Device privacy settings as a tool for protecting consumers

Given the sensitivity of the information that can be exposed when using electronic devices, privacy settings are extremely important tools for consumers, providing them some modest measure of control over the flow of their information.

Microsoft details the privacy settings available for Windows and how they work:

² Zuboff, Shoshana, *You Are the Object of a Secret Extraction Operation* (November 12, 2021) The New York Times, <https://www.nytimes.com/2021/11/12/opinion/facebook-privacy.html>.

³ Press Release, *FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices* (January 17, 2025) FTC, <https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer>.

Windows privacy settings let you control which apps can access your personal data and device features – such as your location, camera, microphone, contacts, and calendar – so you can decide what information apps can use and when.

...

Each privacy setting controls access to a specific type of data, such as your location, camera, or contacts. You can turn access on or off for individual apps.

If you turn off access for an app, that app can't use the related data or feature.⁴

Identifying the growing importance of privacy to consumers, Apple has instituted a number of more protective privacy settings for users. For example, these settings can limit data tracking by applications downloaded to consumer devices:

App Tracking Transparency

Your devices carry the story of your life. We believe you should have a choice in how apps track and share your data with other companies for advertising or with data brokers.

Starting with iOS 14.5 and iPadOS 14.5, apps are required to ask your permission when they want to track you across apps and websites owned by other companies. You can change your preference for any app or prevent apps from asking for permission entirely in Settings.⁵

This bill seeks to ensure consumers' configuration of these settings is respected. It prohibits an operating system or an application from undoing a user's affirmative configuration of a privacy setting without the user's consent. While this protection only applies to settings that a user affirmatively configures, rather than those privacy settings that may be the default, it provides some additional layer of protection for consumers.

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 consent. The overwhelming majority of Californians strongly desire data minimization. However, many software systems and apps change user's privacy settings, most notably after an update. 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

⁴ Microsoft, *Windows privacy settings that apps use*, <https://support.microsoft.com/en-us/windows/windows-privacy-settings-that-apps-use-8b7f2cf4-c359-bf99-0f69-2123cc9ddfc1>.

⁵ Apple, *Control is yours*, <https://www.apple.com/privacy/control/>.

it was prior to the update. AB 2561 would prioritize user's privacy rights and ensure they remain in control of their data.

SUPPORT

None received

OPPOSITION

None received

RELATED LEGISLATION

SB 923 (Becker, 2026) expands consumers' right to deletion of their personal information pursuant to the California Consumer Privacy Act (CCPA) and requires specified online businesses to provide consumers an online method for exercising rights under the CCPA. SB 923 is being heard in this Committee on the same day as this bill.

SB 361 (Becker, Ch. 466, Stats. 2025) expanded the disclosures that data brokers must make when registering with California's Data Broker Registry.

AB 566 (Lowenthal, Ch. 465, Stats. 2025) requires browsers to include functionality configurable by a consumer that enables the browser to send an opt-out preference signal to a business with which a consumer interacts through the browser.

AB 656 (Schiavo, Ch. 464, Stats. 2025) requires large social media platforms to provide users with a clear and accessible mechanism for deleting their accounts and associated personal information.

PRIOR VOTES:

Assembly Floor (Ayes 77, Noes 0)

Assembly Privacy and Consumer Protection Committee (Ayes 15, Noes 0)
