
THIRD READING

Bill No: AB 2561
Author: Valencia (D)
Amended: 4/23/26 in Assembly
Vote: 21

SENATE PRIV., DIGITAL TECH. & CONS. PROT. COMMITTEE: 9-0, 6/8/26
AYES: Cabaldon, Jones, Gonzalez, McNerney, Ochoa Bogh, Padilla, Reyes,
Umberg, Wiener

ASSEMBLY FLOOR: 77-0, 5/14/26 - See last page for vote

SUBJECT: Operating systems and applications: privacy settings

SOURCE: Author

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.

ANALYSIS:

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.

Background

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

This bill is author sponsored. No timely support or opposition has been received.

Comments

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:

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.¹

¹ 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>.

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.²

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

FISCAL EFFECT: Appropriation: No Fiscal Com.: No Local: No

SUPPORT: (Verified 6/9/26)

² Apple, *Control is yours*, <https://www.apple.com/privacy/control/>.

None received

OPPOSITION: (Verified 6/9/26)

None received

ASSEMBLY FLOOR: 77-0, 5/14/26

AYES: Addis, Aguiar-Curry, Ahrens, Alanis, Alvarez, Ávila Farías, Bains, Bauer-Kahan, Berman, Boerner, Bonta, Bryan, Calderon, Caloza, Carrillo, Castillo, Chen, Connolly, Davies, DeMaio, Dixon, Elhawary, Ellis, Flora, Fong, Gabriel, Gallagher, Garcia, Gipson, Jeff Gonzalez, Mark González, Hadwick, Haney, Harabedian, Hart, Hoover, Irwin, Jackson, Johnson, Kalra, Krell, Lackey, Lee, Lowenthal, Macedo, McKinnor, Muratsuchi, Nguyen, Ortega, Pacheco, Papan, Patel, Patterson, Pellerin, Petrie-Norris, Quirk-Silva, Ramos, Ransom, Michelle Rodriguez, Rogers, Blanca Rubio, Sanchez, Schiavo, Schultz, Sharp-Collins, Solache, Soria, Stefani, Ta, Tangipa, Valencia, Wallis, Ward, Wicks, Wilson, Zbur, Rivas

NO VOTE RECORDED: Arambula, Bennett, Celeste Rodriguez

Prepared by: Christian Kurpiewski / P., D.T., & C.P. / (916) 651-1548
6/10/26 16:58:22

**** **END** ****