March 28, 2026

The Honorable Rebecca Bauer-Kahan
Chair, Assembly Committee on Privacy and Consumer Protection
1020 N Street, Room 162
Sacramento, CA 95814

RE: AB 2561 (Valencia) – Operating Systems and Applications: Privacy Settings – **Oppose**

Dear Chair Bauer-Kahan,

On behalf of TechNet and the undersigned organizations, we write to respectfully oppose AB 2561 (Valencia), a bill that would create privacy-protective default settings for users and prohibit changes to these settings without explicit user consent.

We appreciate the author's goal of strengthening consumer privacy protections and ensuring that users maintain meaningful control over their data. AB 2561, however, raises significant concerns regarding operational feasibility, unintended consequences for security and safety, and conflicts with existing privacy frameworks, particularly by requiring that all default settings be configured to the "most privacy protective" option and prohibiting changes without explicit user consent.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of American innovation by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes more than 100 dynamic American businesses ranging from startups to the most iconic companies on the planet and represents five million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

Tension Between Privacy, Security, and Safety

Let us be clear, there is no universally accepted definition of "the most privacy-protected setting." A central concern with AB 2561 is that it presumes a single, uniform "most privacy protective" setting exists across all contexts. However, in practice, privacy, security, and safety are often interdependent and require balanced, context-specific configurations.

For example, protecting users from phishing, malware, and account compromise often requires collecting and analyzing additional signals about user activity. Enhanced security features—such as advanced browsing protections or threat detection systems—may require more data processing than baseline privacy settings, but are essential to protecting users from increasingly sophisticated threats.

A rigid requirement to default to the most restrictive data settings could therefore reduce visibility into harmful activity and weaken user protections, creating a paradox where efforts to increase privacy may inadvertently undermine user safety.

Additionally, depending on a person's perspective, the risks of privacy breaches by malicious actors spreading malware and phishing scams might lead some to choose the most privacy-protective setting, which involves increased monitoring. Conversely, others may be more concerned about the amount of information the service provider has access to, regardless of how that information is used. Therefore, the bill's use of the term "most privacy protective" does not clearly guide the companies on how to comply.

Departure from Established California Privacy Frameworks

AB 2561 represents a significant departure from California's existing privacy framework. Under current law, consumers are provided with meaningful rights and controls, including the ability to opt out of the sale or sharing of personal information, but those frameworks were carefully designed to avoid mandating rigid default configurations across all technologies.

In particular, prior legislative efforts, AB 566 (Lowenthal, 2025) specifically, TechNet and others worked with the author's office and CalPrivacy to reach a neutral position. We are very concerned about anything that might backtrack on some of the elements that helped get us to that position. The negotiations intentionally avoided requiring browser or system-level controls to default to the most restrictive "opt-out" settings. Requiring all systems and applications to default to the most privacy-protective configuration would constitute a substantial shift in California law, with broad implications across the digital economy. It would also fundamentally alter the balance struck by the CPRA, approved by California voters, by dramatically altering the viability of the ad-supported internet, putting consumers at increased risk of a further onslaught of paywalls protecting previously free, ad-supported publications and content.

Operational and Functional Impacts

The bill's requirements could also disrupt core functionality that consumers rely on every day. For example, blocking third-party cookies or similar technologies by default may break embedded content, such as videos, payment tools, or interactive features commonly used across news and media websites.

Certain product features that depend on interoperability across services may not function properly without appropriate data-sharing configurations. These effects may not always be apparent to users and could degrade the overall user experience while providing only a limited incremental privacy benefit.

Comparably, certain safety-critical features rely on limited, purpose-driven access to data. Emergency location services, for instance, may temporarily enable location sharing in order to assist first responders during emergencies. A default configuration that disables such capabilities could delay response times and create real-world safety risks.

Constraints on Security and Product Improvements

AB 2561 would also prohibit changes to a user's privacy settings without explicit consent. While intended to protect users, this provision may unintentionally limit the ability of companies to respond to security threats or improve privacy protections over time.

For example, companies may be unable to automatically implement stronger protections in response to suspicious account activity, such as requiring additional authentication steps like 2FA.

Efforts to reduce data retention periods or enhance privacy defaults may be constrained if such changes require individualized consent before being applied. This creates a scenario where companies could be prevented from implementing more protective or safer configurations, undermining both privacy and security objectives.

These constraints are especially challenging for AI-powered assistants and chatbot systems, which depend on contextual awareness, adaptive safety features, and ongoing monitoring to operate effectively and safely. Limiting the ability to analyze signals in real time—such as those indicating self-harm, fraud, or other high-risk interactions—may weaken built-in safeguards, hinder the ability to intervene properly, and impair system performance by reducing context retention and response quality. Furthermore, requiring personalized user consent before implementing updated safety or monitoring measures could delay the deployment of critical protections, leaving users exposed to new harms and limiting these systems' capacity to adapt in real time.

Scope and Application

The bill does not clearly specify when or how its requirements apply, such as whether they apply only to new users or also to existing users across devices and updates. This lack of clarity creates uncertainty for implementation and raises concerns about inconsistent application across platforms and use cases.

Additionally, the bill may create complications for enterprise-managed devices, educational environments, and other contexts where settings are configured to balance privacy, security, and organizational requirements.

We share the author's commitment to protecting consumer privacy and ensuring transparency and user control. However, AB 2561's approach, requiring a uniform "most privacy protective" default and restricting the ability to adapt settings, does not adequately account for the real-world interplay between privacy, security, and safety.

Without greater flexibility and clarity, the bill risks weakening critical security protections, disrupting widely used digital services, and creating unintended consequences for consumers and businesses alike.

For these reasons, TechNet and the undersigned organizations, respectfully oppose AB 2561 and look forward to working with the author and Committee to develop a more balanced approach that advances privacy while preserving security, safety, and functionality.

TECHNET
THE VOICE OF AMERICAN INNOVATION

If you have any questions regarding our position, please contact Robert Boykin at rboykin@technet.org or 408.898.7145.

Sincerely,

Robert Boykin
Executive Director for California and the Southwest
TechNet

Ronak Daylami, California Chamber of Commerce
Aodhan Downey, Computer and Communications Industry Association