INSIGHTS ASSOCIATION

TECHNET
THE VOICE OF AMERICAN INNOVATION

SIIA

CalChamber

CCIA
Computer & Communications Industry Association
Open Markets. Open Systems. Open Networks.

CIVIL JUSTICE
ASSOCIATION OF CALIFORNIA

May 6, 2026

Assembly Appropriations Committee
California State Capitol
1315 10th St
Sacramento, CA 95814

Re: AB 2169 - "Digital Choice Act" (Oppose)

Dear Chair Wicks and Members of the Assembly Appropriations Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose AB 2169. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] Proposed regulations on the intrastate provision of digital services therefore can have a significant, nationwide impact on CCIA members.

While CCIA supports robust consumer protections and sound competition policy, the proposed bill negatively impacts consumer privacy and security online, raises First Amendment concerns, and imposes technically infeasible requirements on covered businesses. These impacts outweigh any small improvement in convenience that data portability might bring consumers.

[1] For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.

Forced data interoperability undermines online privacy and data security.

Although AB 2169 requires that "A social media company or model operator shall reasonably secure a user's personal information, contextual data, or social graph obtained through an interoperability interface" and may not "share or receive a user's personal information, contextual data, or social graph through the interoperability interface without the user's consent," the interoperability interface's very existence undercuts user privacy. In particular, widespread consumer privacy rights like data deletion become nearly impossible to implement under such conditions: once a third party possesses a user's data, ensuring its deletion is generally infeasible.

The bill also undermines user discretion. Social media allows for a substantial amount of personal information to be shared between users, such as the existence of a connection, shared media, and communications. However, AB 2169 appears to require that a service enable the extraction and sharing of that data irrespective of the preferences of other connected users who have not chosen to move their data to another platform.

Moreover, a public-facing interface designed for the purpose of extracting user data significantly increases the risk of data breaches. A hacker or foreign adversary accessing such an interface could obtain data from many social media users across several sites. In other key industries such as healthcare, interoperability of records has significantly increased vulnerability to cyberattacks in recent years.[2]

Different companies have different security practices. Some encrypt data while others do not. Companies also retain different types of data for different periods of time, and are bound by different laws and regulations if they operate across multiple jurisdictions, as online services tend to do. Many also tailor their security practices to the specific types of data they process. AB 2169 undermines companies' ability to create the best security features for their specific data uses, which in turn undermines their users' safety.

While AB 2169 might save consumers a modicum of time when setting up a profile on a new social media site, the potential time saved is not worth the security risks. Companies should be allowed to protect their users' information in the best way possible given the configuration of their own websites without needing to water down such practices to make user data accessible to other companies.

AB 2169 gives the Attorney General overbroad regulatory authority

AB 2169 offers the centralization of technical authority within a political office, effectively shifting the responsibility for internet architecture from global engineering bodies to a single state executive. Historically, the "open protocols" that power the internet have been developed through a voluntary, consensus-based, multi-stakeholder process involving organizations like the Internet Engineering Task Force (IETF).[3] By granting the Attorney General the power to "assess" and "identify" which protocols are acceptable, the state creates a permissioned

---

[2] *See, e.g.*, Lancer Gates, *Cyber Attacks on Interoperable Electronic Health Records: A Clear and Present Danger*, 121 Mo. Med. 6, 6-9 (2024), https://pmc.ncbi.nlm.nih.gov/articles/PMC10887471/.

[3] Harald Alvestrand, *RFC 3935: A Mission Statement for the IETF*, Internet Engineering Task Force (Oct. 2004), https://www.rfc-editor.org/info/rfc3935.

innovation environment. This could lead to a stagnation in data security, where companies are discouraged from developing superior, more secure, or more private proprietary methods because they do not fit the government's pre-approved list. Such a mandate effectively turns the Attorney General into a Chief Technology Officer for the private sector, stifling the industry's ability to evolve past current standards.

Furthermore, this provision introduces systemic cybersecurity risks by forcing a digital "monoculture." Cybersecurity experts often note that diversity in software and protocols is a vital defense mechanism; if every social media platform and AI model is legally compelled to use the same government-vetted protocols, a single vulnerability in that protocol could expose the entire digital ecosystem simultaneously.[4] As noted by critics at the Reason Foundation, mandatory interoperability often ignores the security practices of the receiving parties. By stripping companies of their ability to vet the security of the "pipes" through which they send sensitive "contextual data" and "social graphs," the bill may force businesses to facilitate data transfers that they know to be insecure, solely to remain in compliance with the Attorney General's regulatory list and provisions found in AB 2169.[5]

CCPA already offers existing consumer rights for data portability.

AB 2169 is fundamentally unnecessary given the existing legal and technical landscape. Under the California Consumer Privacy Act (CCPA), consumers already possess a robust right to data portability,[6] one that has been operative for years and has driven meaningful industry compliance. Major technology providers have not merely met these requirements but exceeded them through sophisticated, voluntary tools developed in direct response to consumer demand. Google Takeout, Apple's Data & Privacy portal, and Meta's Download Your Information tool reflect the same dynamic: companies innovating on portability because their users expect it, not because a legislature prescribed it.

The Data Transfer Initiative (DTI) is a collaboration between major technology firms designed to enable seamless, service-to-service data transfers.[7] Unlike a simple data download, DTI facilitates direct, real-time transfers between platforms, allowing a user to migrate content from one service to a competitor without downloading a file locally. This represents exactly the kind of frictionless portability that the bill seeks to achieve, built entirely through engineering consensus rather than legislative mandate.

In contrast to these frameworks, AB 2169 imposes a rigid, state-mandated architecture that adds to compliance burdens without providing a clear benefit to consumers. The better policy is to enforce the CCPA's existing portability rights while allowing industry-led initiatives like DTI to mature, rather than intervening where the market is already serving consumers.

---

[4] Aspen Hopkins et al., *Recourse, Repair, Reparation, & Prevention: A Stakeholder Analysis of AI Supply Chains*, FAccT '25: Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency, June 23, 2025, at 209, https://doi.org/10.1145/3715275.3732017.

[5] Jen Sidorova, *Top 3 Cybersecurity Priorities for the Trump Administration*, Reason Found. (May 20, 2025), https://reason.org/commentary/top-3-cybersecurity-policy-priorities-for-the-trump-administration/.

[6] Cal. Civ. Code § 1798.130(a) (West 2018).

[7] Data Transfer Initiative, https://dtinit.org/.

Requiring covered businesses to display content against their wishes violates the First Amendment.

In 2024, the Supreme Court ruled that "The government may not, in supposed pursuit of better expressive balance, alter a private speaker's own editorial choices about the mix of speech it wants to convey."[8] However, AB 2169 requires that covered businesses allow users to "Share a covered user's social graph or user-selected parts of the social graph to a social media platform designated by the user." This provision effectively requires the receiving business to display this portion of the social graph whenever another site's user requests that they do so. In essence, internet users from another website would have veto power over a covered business's community standards and content moderation practices. Such a requirement is an unconstitutional "intrusion on protected editorial discretion."[9] It compels speech without regard to the multi-faceted design decisions platforms make about which product features to offer based on the type of service they want to have, the risks and benefits of specific features, how those features help the platform achieve its objectives, and a host of legal, privacy, safety, financial and other considerations that accompany such decisions.

The bill contains technically infeasible requirements.

Besides undermining privacy, data security, and free speech, AB 2169's requirements are not technically feasible. Open protocols for interoperability across many websites that have been proven to securely operate at scale do not yet exist. Industry standards have not yet been developed for building such projects, and without tested protocols for keeping user data safe, such requirements will jeopardize privacy further.

Moreover, making legacy systems compatible with such an interface is an enormous undertaking. Legacy models are often built with many assumptions regarding security protocols, access controls, and user experience, and every part of a covered website relating to any of these features might have to be redesigned. For example, forced interoperability risks exposing proprietary data to external systems. Even if this could be done safely, the protocols for such transfers would need to be revised with every significant modification of the interoperability interface. Security and access controls would also be jeopardized, since an interoperability interface requires that websites allow interactions with a wide swath of the internet and can thus no longer rely on protocols that trust information only from a limited number of sources. User experience would also suffer, as websites' technical features are often optimized for their expected traffic flow, which would become unpredictable. Companies would also lose their ability to tailor their websites' interfaces to their specific user bases. In sum, it would not be possible for many websites to maintain their current customer service standards under such a law.

Costs to the State

The implementation of AB 2169 presents a substantial and unquantified fiscal burden on the State of California by shifting the responsibility for internet architecture from global engineering bodies to a state executive office. Defending this statute against inevitable constitutional challenges—specifically regarding the "intrusion on protected editorial

[8] *Moody v. NetChoice*, 144 S. Ct. 2383, 2403 (2024).
[9] *Id.* at 2398.

discretion" and First Amendment violations recognized in *Moody v. NetChoice*[10]—will require millions of dollars in General Fund expenditures for protracted litigation and outside counsel.

Furthermore, the bill's requirements prescribed to the Attorney General's offices necessitates a massive expansion of the Department of Justice to include specialized software engineers and data scientists to "assess" and "identify" acceptable open protocols. This regulatory expansion mirrors the significant fiscal pressures identified in the analysis of SB 1047 (2024)[11], which required tens of millions of dollars for expert staffing to oversee AI safety frameworks. Additionally, the mandate to designate open protocols is technically infeasible as secure standards at this scale do not yet exist, forcing the State to fund novel technical research that is historically handled by voluntary, multi-stakeholder processes like the IETF. Similar to the fiscal warnings in AB 1757 (2023) regarding web accessibility standards, this creates significant administrative overhead.

Beyond administrative growth, the bill introduces systemic fiscal risks by creating a novel vector for mass consumer fraud. By mandating a "third-party-accessible interoperability interface", AB 2169 provides a centralized target for bad actors to weaponize account takeover attacks at scale. Fraudsters could exploit these interfaces to port vast amounts of "contextual data" and "social graphs"—sensitive information that reflects a user's connections and interactions—directly to malicious platforms to defraud California consumers. In 2025 alone, account takeover rates accelerated by 37%[12], with phishing and identity-based attacks becoming the primary tools for financial loss[13]. Forcing companies to facilitate data transfers through potentially insecure "pipes" they cannot vet increases the State's liability for investigation and remediation. The fiscal impact of combatting such risk is immense; previous data breach settlements in California highlight the high costs of privacy enforcement and consumer restitution. If state-mandated protocols lead to large-scale data breaches or facilitate fraud—risks already observed in interoperable healthcare records—the State would face escalating costs related to consumer protection enforcement, identity theft mitigation, and a significant judicial backlog.

* * * * *

Sincerely,

Aodhan Downey
State Policy Manager, West Region
Computer & Communications Industry Association

[10] *Moody v. NetChoice*, 144 S. Ct. 2383, 2403 (2024).
[11] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB1047
[12] "H1 2025 Update: State of Omnichannel Fraud." *TransUnion Canada*, 2025.
[13] Cvetko, Jana. "Microsoft Digital Defense Report 2025 – Cybersecurity Trends & Threats." *Source EMEA*, 22 Oct. 2025.

On Behalf of:

Ronak Daylami, California Chamber of Commerce
Annalee Augustine, Civil Justice Association of California
Howard Fienberg, Insights Association
Abigail Wilson, Software Information Industry Association
Robert Boykin, TechNet