Date of Hearing: April 21, 2026
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Josh Lowenthal, Chair
AB 2169 (Lowenthal) – As Introduced February 18, 2026

PROPOSED AMENDMENTS

SUBJECT: Social media platforms: artificial intelligence models

SYNOPSIS

Social media platforms have been a force for good in many ways, providing spaces for community, enabling users to stay connected with friends, and allowing many to build small businesses. However, not everyone has benefited equally. For some, the constant stream of content and pressure to stay connected has become overwhelming, leading them to want to leave these platforms entirely. Others may wish to leave a particular platform, rather than abandoning social media altogether. Yet, social media companies often make it difficult for these users to transition between platforms. Unlike email platforms, social media platforms generally lack "interoperability." A Gmail user and a Microsoft Outlook user can easily communicate with one another, despite utilizing different platforms. A Facebook user and an X user cannot – when a user chooses to leave a platform, they leave behind their network of connections.

This bill seeks to make the process of cutting ties with the largest social media platforms easier by requiring that social media platforms become interoperable. The bill would allow a user of a platform to request all of their data, including their "social graph", be provided to them in a format that allows it to be uploaded on another platform. In addition, it requires platforms to allow users to post across platforms simultaneously. The author and sponsor, Project Liberty, argue that requiring interoperability will create more competition and result in platforms improving as other platforms with better practices attract users.

Committee amendments, enumerated in Comment # 9, allow users to request the deletion of all of their data, including their social graph; prohibit the operators of third-party interfaces from collecting or using any of the data they are helping to transfer; and clarify that platforms only have to implement what is technically feasible.

This bill is sponsored by Project Liberty and enjoys the support of a number of tech safety groups and child safety groups, including Tech Equity and the Anxious Generation Foundation. A coalition of business associations, including the California Chamber of Commerce and TechNet, opposes the bill.

EXISTING LAW:

1) Requires a social media platform to provide a clear and conspicuous button that enables the user to delete their account that meets both of the following:

    a. Is clearly and conspicuously placed as an immediately visible option in the social media platform's settings menu with the words "Delete Account."

b. The settings menu containing the button is accessible in the application, on a browser, or on any other format that a user can use to access the social media platform. (Civ. Code § 3273.90 (a).)

c. Prohibits a social media platform from obstructing or interfering with a user's ability to delete their account, including, but not limited to, by using dark patterns. (Civ. Code § 3273.90 (b).)

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. (Civ. Code § 1798.100 *et seq*.)

3) Establishes the California Privacy Rights Act of 2020 (CPRA), which amends the CCPA and creates the California Privacy Protection Agency (Privacy Agency), which is charged with implementing these privacy laws, promulgating regulations, and carrying out enforcement actions. (Civ. Code § 798.100 *et seq*.; Proposition 24 (2020).)

4) Provides consumers with the right to request that a business delete any personal information about the consumer which the business has collected from the consumer. (Civ. Code § 1798.105(a).)

5) Defines "business" as:

a. A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

i. As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year, as adjusted pursuant to subdivision (d) of Section 1798.199.95.

ii. Alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers or households.

iii. Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.

b. Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business and with whom the business shares consumers' personal information. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common

branding" means a shared name, servicemark, or trademark that the average consumer would understand that two or more entities are commonly owned.

c. A joint venture or partnership composed of businesses in which each business has at least a 40 percent interest. For purposes of this title, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.

d. A person that does business in California, that is not covered by paragraph (i), ii), or (iii), and that voluntarily certifies to the California Privacy Protection Agency that it is in compliance with, and agrees to be bound by, this title.

6) Defines "consumer" as a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier. (Civ. Code § 1798.140(i).)

7) Defines "dark pattern" as a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation. (Civ. Code § 1798.140(l).)

8) Defines "personal information" 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." It does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. (Civ. Code § 1798.140(v).)

9) Defines "artificial intelligence model" as an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments. (Bus. & Prof. Code § 22717.11 (b).)

10) Defines "social media company" as a person or entity that owns or operates one or more social media platforms. (Bus. & Prof. Code § 22675 (e).)

11) Defines "social media platform" as a public or semipublic internet-based service or application that has users in California and that meets the following criteria:

a. A substantial function of the service or application is to connect users in order to allow users to interact socially with each other within the service or application. A service or application that provides email or direct messaging services shall not be considered to meet this criterion on the basis of that function alone.

b. The service or application allows users to do all of the following:

i. Construct a public or semipublic profile for purposes of signing into and using the service or application.

ii. Populate a list of other users with whom an individual shares a social connection within the system.

iii. Create or post content viewable by other users, including, but not limited to, on message boards, in chat rooms, or through a landing page or main feed that presents the user with content generated by other users. (Bus. & Prof. Code § 22675 (f).)

12) Permits amendment of the CPRA by a majority vote of each house of the Legislature and the signature of the Governor provided such amendments are consistent with and further the purpose and intent of this act as set forth therein. (Proposition 24 § 25 (2020).)

THIS BILL:

1) Defines the following terms:

a. "Artificial intelligence model" has the meaning defined in Section 22757.11 of the Business and Professions Code.

b. "Business" has the meaning defined in Section 1798.140 of the Civil Code.

c. "Consumer" has the meaning defined in Section 1798.140 of the Civil Code.

d. "Contextual data" means:

i. Information provided by a user to an artificial intelligence model and any context or derivative data associated with the user's interactions with the artificial intelligence model, including prompts, conversational histories, files, preferences, metadata, and any model-generated or inferred data linked to or generated from those interactions.

ii. "Contextual data" does not include a model operator's trade secrets.

e. "Model operator" means:

i. A person that deploys an artificial intelligence model, including under license or contract.

ii. "Model operator" does not include a person that interacts with artificial intelligence models solely through application programming interfaces, licensed services, prompting, or fine tuning.

f. "Open protocol" means a publicly available set of rules that enables interoperability and data exchange between social media platforms or model operators by providing a common data infrastructure by which multiple social media platforms or model operators can access a user's personal information that is free from licensing fees and patent restrictions.

g. "Personal information" means any information that identifies or describes an individual.

h. "Social graph" means data that represents a person's connections and interactions within a social media platform, including all of the following:

   i. The person's social connections with other users

   ii. Content created by the person.

   iii. The person's responses to other users' content, including comments, reactions, mentions, reposts, shares, and other responses.

   iv. Other users' responses to the person's content.

   v. Metadata associated with any of the items described in subparagraphs (ii) to (iv), inclusive.

   vi. Relational references sufficient to maintain the associations among data elements in the items described in subparagraphs (i) to (v), inclusive.

i. "Social graph" does not include another user's or an entity's content and responses that have been designated private by those users and entities, including private messages.

j. "Social media company" has the meaning defined in Section 22675 of the Business and Professions Code.

k. "Social media platform" has the meaning defined in Section 22675 of the Business and Professions Code.

2) Requires a social media company or model operator to, at the request of a consumer, provide that consumer with a copy of their personal information, contextual, and social graph within five days of the request being made.

3) Requires that personal information be provided in a format that is all of the following:

   a. Portable, to the extent technically feasible.

   b. Readily usable to the extent practicable.

   c. In a form that allows the consumer to transmit the data to another social media platform or model operator without impediment if the platform or model operator processes the data by automated means.

4) Requires a social media company to implement a transparent, third-party-accessible interoperability interface that allows a user to choose both of the following:

   a. Share a consumer's social graph or consumer-selected parts of a social graph to a social media platform designated by the consumer.

   b. Enable a third party to, with the consumer's permission, access a social graph created by the consumer and be notified when a new or updated social graph is available.

5) Requires a model operator to implement a third-party-accessible interoperability interface to allow a consumer to share their contextual data directly with the other artificial intelligence models and enable those models to be notified when new or updated data is available.

6) In order to comply with the requirements, a social media company or model operator shall do the following:

    a. Utilize and open protocol.

    b. Facilitate and maintain interoperability and continuous real-time data sharing with other platforms and models through an interoperability interfaced based on reasonable terms that do not discriminate.

    c. Disclose to other social media companies and model operators complete, accurate, and regularly updated documentation describing access to the interface.

7) Requires a social media company or model operator to reasonably secure a user's personal information, contextual data, or social graph obtained through an interoperability interface.

8) Requires a business that accesses and interoperability interface to take steps to meet platform integrity standards, including data security, data privacy, and abuse mitigation practices.

9) Prohibits a social media company, model operator, or other controller sharing or receiving a user's personal information, contextual data, or social graph through the interoperability interface without the consumer's consent.

10) Requires a social media company or model operator adopt an accessible, prominent, and persistent method for users to give consent for data sharing with other platforms or model operators.

11) States that a social media company is not required to do any of the following:

    a. Provide access to inferences, analyses, or data that the company generated internally about the user and proprietary algorithms, ranking systems, or other internal operating mechanisms.

    b. Transmit personal information, contextual data, or a social graph that is stored or structured in a proprietary format and with respect to those three elements both of the following apply:

        i. An open, industry standard format is not reasonably available.

        ii. Transmitting the elements would disclose proprietary information.

12) Requires a business that uses an AI model provided by a model operator to provide and application or service to a consumer to promptly transmit a consumers request to the model operator with sufficient information for the operator to execute the request and communicate with the consumer.

13) Authorizes the Attorney General to adopt regulations identifying specific open protocols.

14) Creates a rebuttable presumption if a company uses an open protocol that the Attorney General has identified.

15) Provides for enforcement by the Attorney General.

COMMENTS:

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

> AB 2169 would establish the Digital Choice Act, requiring social media and AI companies to provide users, upon request, with a copy of their personal information, contextual data, and social graph. Companies must fulfill these requests within five business days and deliver the data in a format that is readily transferable and usable, where technically feasible.
>
> The bill is intended to empower users while promoting innovation and competition. By enabling meaningful data portability, AB 2169 encourages platforms to compete on the quality and safety of user experiences rather than relying primarily on engagement-driven advertising. In doing so, it creates a pathway for greater user control, fosters innovation, and creates more enriching online environments.

2) **Discontent creators.** Social media has grown immensely over the past two decades, now encompassing everything from social networking to forums, chat rooms, content-sharing platforms, and even job-seeking tools. With its wide range of functionalities, over 80% of Americans are active on at least one platform.[1] Recent reports show that the average American spends nearly 2.5 hours per day on social media.[2] People turn to these platforms for a variety of reasons; some use them as news and information sources, others to grow small businesses, and many to maintain relationships and build community. Social media has even given rise to a new economic model in the form of influencers and the attention economy.

However, the benefits of social media are not universal. Many users feel compelled to stay online out of fear of missing out, only to find themselves losing valuable time to mindless scrolling instead of meaningful social interaction. Other users enjoy spending time on social media as a whole but may wish to transition to a new platform. Unfortunately, social media platforms often make this process exceedingly difficult. It is not currently possible for a Facebook user to easily migrate their network of connections to X, and it is not possible for an X user to communicate directly with a user on Facebook. Social media platforms are designed as self-contained, self-sufficient ecosystems. Choosing to leave a platform involves abandoning one's carefully cultivated social network, with no guarantee that their network can be reconstructed on the other end. This is especially problematic for individuals who monetize their social media presence: the barrier for influencers to leave a platform is high, as they cannot bring their followers or content with them.

This bill is designed to help discontent creators shift everything they have built on one social media platform to another social media platform.

---

[1] Jeffrey Gottfried, "Americans' Social Media Use", *Pew Research Center* (Jan. 31, 2024), https://www.pewresearch.org/internet/2024/01/31/americans-social-media-use/.
[2] Robin Geuens, "What is the average time spent on social media each day?", *Soax* (Sept. 5, 2024), https://soax.com/research/time-spent-on-social-media.

3) **Utah's Digital Choice Act.** In 2025, Utah passed their Digital Choice Act[3], which was updated in 2026 to modify several provisions and delay implementation until July 1, 2027.[4] Opponents of this bill believe that there will be a third bill in 2027 to modify more provisions in an attempt to make the bill workable.

Substantially similar to this bill, Utah's Digital Choice Act essentially allows consumers to request portable copies of their data, which includes contextual data and their social graph, that they can upload into a different platform to populate their profiles with all of their posts, connections, and interests so they do not need to start over on the new platform. Once requested, a platform has five days to provide the data.

In addition, social media platforms are required to implement transparent, third-party-accessible interoperability, that allows users to transfer their social graph to another social media platform, or their contextual data directly to other AI models.

Finaly, Utah's law requires the development of an interoperable system that allows users to post simultaneously across platforms and transparent and third-party-accessible. According to Project Liberty, the sponsors of the bill and the developer of the Decentralized Social Networking Protocol (DSNP), an open data protocol that meets the definition of a transparent third party, social media interoperability much like the open standards that make email or the web function seamlessly, will allow individuals to control access to their own data across platforms. They argue that this will increase competition and the pressure on companies to improve their platforms, rather than the current race to the bottom, because it allows users to move their information to safer, healthier, and perhaps more advantageous digital spaces.

4)**What is interoperability?** Researchers explain interoperability this way:

> Interoperable systems refer to the ability of different technological systems, platforms, or devices to work together effectively, enabling them to exchange and process information in a standardized manner. These systems are designed to overcome technical barriers and ensure that distinct software, hardware, or networks can collaborate to achieve common objectives. Interoperability is essential in achieving operational efficiency, reducing redundancies, and enhancing the flow of information across diverse environments.[5]

5) **The social graph.** A social media graph can be thought of as a web or a map that contains a person's entire online life on a platform. It is all of their connections, the things they have liked or disliked, their posts, their purchases, whose posts they have commented on, and users who have commented on their posts. Essentially it is anyway that they have interacted on the platform since they created their account. Think of it as a bulletin board in a detective procedural on television that includes pictures, notes, evidence, places, and news articles all with a red string connecting those items on the board with the victim of a crime and each other. That is a social graph, and, in this case, it is all attached to the user rather than a victim.

---

[3] H.B. 418 (Fiefia, 2025) https://le.utah.gov/~2025/bills/static/HB0418.html.
[4] H.B.408 (Fiefia, 2026) https://le.utah.gov/~2026/bills/static/HB0408.html.
[5] Agumalu, Sandra & Augustine, Chibueze & Alonge, Mayowa & Joseph, Oloyede. *Privacy and Security in Interoperable Systems* (2025). https://www.researchgate.net/publication/387948506_Privacy_and_Security_in_Interoperable_Systems.

This bill would require that the entire bulletin board that conceivably was built over a decade or more be bundled into a transportable package where it is automatically reconstructed in the exact same way in a new place.

6) **Why interoperability?** Open Future, an organization in the European Union that advocates for an open internet, describes the benefits of interoperability this way:

> The dramatic increase in the power of commercial online platforms has been one of the main outcomes of the digital transition so far. The internet is dominated by a few platforms that have, over the years, gained a monopolistic position over online ecosystems. Platformization has upended the vision of a neutral and open internet.
>
> The modern internet consists largely of closed, private communication spaces under corporate control. Platforms are the gatekeepers of content, communications, and data flows. This challenge is often framed in economic terms as affecting competition and innovation among business users and choice for end users. It also has negative societal effects, leading to social polarization, the spread of misinformation, censorship, or the growth of social inequalities.
>
> [. . .]
>
> [I]nteroperability is a design principle at the heart of the original vision for the open internet. In technical terms, the principle means the ability of one service to connect to another so that data and content can flow freely.
>
> In the platformized internet, gatekeepers reap the benefits of the interoperable internet without being required to make their own services or data interoperable. That's why interoperability mandates for gatekeeper platforms have great promise. They can open up platforms and ensure open communication flows through them in a way that supports both market competition and the democratization of power that these platforms now hold.[6]

Economic researchers writing for the Yale Journal of Regulation, describes "equitable interoperability" this way:

> "Equitable interoperability" means that an entrant can not only join the platform, but join on qualitatively equal terms as others, without being discriminated against by the dominant platform that might have its own competing service. Equitable interoperability facilitates competition in innovation and differentiation by digital services but entails oversight by a regulator that determines when advances should become part of the regulated interface. It effectively prohibits self-preferencing and discrimination against firms that are not part of the dominant ecosystem.
>
> A simple example is an entering internet service provider (ISP) wishing to join the World Wide Web and its system of interconnection. Such a firm can adopt open standards like TCP/IP and Network Access Points to offer the same functionality as rival ISPs, and, importantly, connect its users to just as large a network size. Similarly, the creation of the

---

[6] *Paradox of Open: Policies for the Digital Commons/A Public, Interoperable Social Media Space*, Open Futures. https://openfuture.eu/policies-for-the-digital-commons/interoperable-social-media/.

> "Open Banking" regulation in the United Kingdom established an interface that licensed financial technology fintech) companies could use, with customer permission, to connect to the bank accounts of their customers. The existence of the banks and their data attracted fintech applications, all of which entered on a level playing field using the same interface. Even the customers of a small bank can have full access, due to that interface, to all participating fintech providers, strengthening competition between banks. By contrast, Google's Android operating system (OS) offers interoperability to entrants, but it does not do so equitably because Google restricts access to various valuable apps and features in the interoperable version of Android OS.[7]

In other words, interoperability is a measure of how compatible different systems are with one another. Email is a digital service with high interoperability. Users of Gmail and Microsoft Outlook can send messages to each other, despite using different platforms. By comparison, users of Facebook cannot send messages directly to users of X – to communicate, they must share a platform. As a result, this creates a high barrier for leaving Facebook or X if all your friends and family are there. You cannot take them with you.

7) **The challenges of interoperability.** Social media interoperability is a concept that has been vexing technologists and regulators for some time. Not only does it raise privacy and cybersecurity concerns, it also raises questions about the best approach to social media interoperability. Should it require platform to platform interoperability or, as in the case of this bill, should it involve a third part to serve as a connector between the platforms?

EU Digital Markets Act. In 2022, the EU adopted the Digital Markets Act (DMA), which is focused on "gatekeepers," which are companies that create bottlenecks between businesses and consumers and have an entrenched position in digital markets after several years of discussion.[8] During the debates on the DMA, the EU considered including social media platform interoperability requirements in the law. However, the final agreement, the DMA was limited to requiring interoperability between direct messaging systems. The DMA allows new messaging services to demand interoperability (the ability to exchange messages) from the internet's largest messaging services (like WhatsApp, Facebook Messenger, and iMessage). But an interoperability requirement for messaging services that are end-to-end encrypted raises particularly thorny security and privacy concerns, and those concerns need to be addressed before interoperability requirements are enforced against those services.[9] Looking into these concerns alone will take years, much less looking to expand the DMA to cover interoperability between the platforms themselves.

Supporting the difficulty of accomplishing this task, associations representing technology companies raise the following concerns:

---

[7] Fiona M. Scott Morton, et al. "Equitable Interoperability: The 'Supertool' of Digital Platform Governance," *Yale Journal of Regulation* (2023) https://economics.yale.edu/sites/default/files/2023-09/p1848.pdf.
[8] Mitch Stoltz, et al. *The EU Digital Markets Act Places New Obligations on "Gatekeeper" Platforms*, Electronic Frontier Foundation (May 2, 2022) https://www.eff.org/deeplinks/2022/04/eu-digital-markets-act-places-new-obligations-gatekeeper-platforms.
[9] Mitch Stoltz, et al. *The EU Digital Markets Act's Interoperability Rule Addresses An Important Need, But Raises Difficult Security Problems for Encrypted Messaging*, (May 2, 2022) https://www.eff.org/deeplinks/2022/04/eu-digital-markets-acts-interoperability-rule-addresses-important-need-raises.

> [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.
>
> 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.
>
> [. . .]
>
> 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.

Given the difficulties the EU has had in implementing interoperability, the technology concerns raised by the companies that will be tasked with implementing these requirements, and the challenges that have arisen in implementing Utah's Digital Choice Act, this bill may be premature. The author may want to consider whether at this stage it might be helpful to convene a working group of experts to determine the best way to achieve interoperability across social media platforms.

8) **Throwing artificial intelligence (AI) into the mix.** As noted in the section outlining what this bill does, it requires that AI model operators, defined as the person who deploys an AI system, to achieve the same level of interoperability as social media platforms. However, in the case of AI models, rather than transferring the social graph, it requires that they allow a consumer to transfer their contextual data, meaning information provided by the user to an AI model and any context or derivative data associated with the user's interactions with model, including prompts, conversational histories, files, preferences, metadata, and any model-generated or inferred data linked to or generated from those interactions.

Unlike social media platforms, which are known to intentionally cultivate walled gardens, whether interoperability between AI models is possible remains an open question. The potential for interoperability among certain AI *systems* is clear – particularly for AI agents (systems capable of acting, not just producing text or images) – but at present, it is unclear how AI models would be made interoperable. The author may wish to consider removing AI models from the bill at this time.

9) **Amendments.** The author has agreed to amendments that ensure that companies are only required to implement the portions of the bill that are technically feasible. In addition, they require social media platforms to delete all of a person's information, including their social graph, at the request of the consumer. The amendments also prohibit and operator of a third-party-accessible interoperability interface from collecting, selling, sharing, or otherwise accessing a consumer's data while transferring it to another platform. Finally, the author has requested that the term "model" be replaced with "deployer." The amendments are as follows:

22589.10. This chapter shall be known as the Digital Choice Act.

22589.11. For purposes of this chapter:

(a) "Artificial intelligence model" has the meaning defined in Section 22757.11.

(b) "Business" has the meaning defined in Section 1798.140 of the Civil Code.

(c) "Consumer" has the meaning defined in Section 1798.140 of the Civil Code.

(d) (1) "Contextual data" means information provided by a user to an artificial intelligence model and any context or derivative data associated with the user's interactions with the artificial intelligence model, including prompts, conversational histories, files, preferences, metadata, and any model-generated or inferred data linked to or generated from those interactions.

(2) "Contextual data" does not include a ~~model operator's~~ ***deployer's*** trade secrets.

(e) (1) "~~Model operator~~ ***Deployer***" ***means a person that makes an artificial intelligence model available to a third party for use, modification, copying, or combination with other software.*** ~~means a person that deploys an artificial intelligence model, including under license or contract.~~

(2) "~~Model operator~~ ***Deployer***" does not include a person that interacts with artificial intelligence models solely through application programming interfaces, licensed services, prompting, or fine tuning.

(f) "Open protocol" means a publicly available set of rules that enables interoperability and data exchange between social media platforms or ~~model operators~~ ***deployers*** by providing a common data infrastructure by which multiple social media platforms or ~~model operators~~ ***deployers*** can access a user's personal information that is free from licensing fees and patent restrictions.

(g) "Personal information" means any information that identifies or describes an individual.

(h) (1) "Social graph" means data that represents a person's connections and interactions within a social media platform, including all of the following:

(A) The person's social connections with other users

(B) Content created by the person.

(C) The person's responses to other users' content, including comments, reactions, mentions, reposts, shares, and other responses.

(D) Other users' responses to the person's content.

(E) Metadata associated with any of the items described in subparagraphs (A) to (D), inclusive.

(F) Relational references sufficient to maintain the associations among data elements in the items described in subparagraphs (A) to (E), inclusive.

(2) "Social graph" does not include another user's or an entity's content and responses that have been designated private by those users and entities, including private messages.

(i) "Social media company" has the meaning defined in Section 22675.

(j) "Social media platform" has the meaning defined in Section 22675 of the Business and Professions Code.

22589.12. (a) A social media company or ~~model operator~~ ***deployer*** shall allow a consumer to request a copy of the consumer's personal information, contextual data, and social graph.

(b) If a consumer requests a copy of the consumer's personal information, contextual data, and social graph pursuant to subdivision (a), a social media company or ~~model operator~~ ***deployer*** shall provide, within five business days, the consumer's personal information, contextual data, and social graph in a format that is all of the following:

(1) Portable to the extent technically feasible.

(2) Readily usable to the extent practicable.

(3) In a form that allows the consumer to transmit the data to another social media platform or ~~model operator~~ ***deployer*** without impediment if the social media platform or ~~model operator~~ ***deployer*** processes the data by automated means.

(c) At the request of a consumer, a social media company shall permanently delete a user's personal information, including the user's social graph, and relational references.

22589.13. (a) ~~A~~ ***To the extent it is technically feasible, a*** social media company shall implement a transparent, third-party-accessible interoperability interface that allows a user to choose to do both of the following:

(1) Share a covered user's social graph or user-selected parts of the social graph to a social media platform designated by the user.

(2) Enable a third party to, with the user's permission, access social graph created by the user and be notified when a new or updated social graph is available.

(b) ~~A~~ ***To the extent it is technically feasible, a*** ~~A model operator~~ ***deployer*** shall implement a third-party-accessible interoperability interface to allow a user to share the user's contextual data directly with other artificial intelligence models as the user designates and enable those artificial intelligence models to be notified when new or updated data is available.

(c) ~~A~~ ***To the extent it is technically feasible,*** ~~T~~ ***t***o comply with subdivisions (a) and (b), a social media company or ~~model operator~~ ***deployer*** shall do all of the following:

(1) Utilize an open protocol.

(2) Facilitate and maintain interoperability and continuous, real-time data sharing with other social media platforms or artificial intelligence models through an interoperability interface based on reasonable terms that do not discriminate.

(3) Disclose to other social media companies or ~~model operators~~ ***deployers*** complete, accurate, and regularly updated documentation describing access to the interoperability interface required under this section.

(d) A social media company or ~~model operator~~ ***deployer*** shall reasonably secure a user's personal information, contextual data, or social graph obtained through an interoperability interface.

(e) A business that accesses an interoperability interface shall take reasonable steps to meet platform integrity standards, including data security, data privacy, and abuse-mitigation practices necessary to preserve user protections and secure any data it acquires, processes, or transmits.

(f) A social media company, ~~model operator~~ ***deployer***, or other controller shall not share or receive a user's personal information, contextual data, or social graph through the interoperability interface without the user's consent.

(g) A social media company or ~~model operator~~ ***deployer*** shall adopt an accessible, prominent, and persistent method for users to give consent for data sharing with other social media platforms or ~~model operators~~ ***deployers*** through the interoperability interface.

(x) A third-party-accessible interoperability interface shall not collect, retain, use, sell, share, or otherwise access consumer data that is being transferred between platforms.

(h) This section does not require a social media company to do any of the following:

(1) Provide access to either of the following:

(A) Inferences, analyses, or derived data that the social media company has generated internally about a user.

(B) Proprietary algorithms, ranking systems, or other internal operating mechanisms.

(2) Transmit personal information, contextual data, or a social graph that is stored or structured in a proprietary format and with respect to that personal information, contextual data, or social graph, both of the following apply:

(A) An open, industry standard format is not reasonably available.

(B) Transmitting the personal information, contextual data, or social graph would disclose information described in paragraph (1).

(i) A business that uses an artificial intelligence model provided by a ~~model operator~~***deployer*** to provide an application or a service to a consumer shall promptly transmit a consumer's request to the ~~model operator~~***deployer*** with sufficient information for the ~~model operator~~***deployer*** to execute the request and communicate about the request with the consumer.

22589.14. (a) The Attorney General may adopt regulations to identify specific open protocols that the Attorney General has determined, after an assessment, meet the definition of "open protocol" listed in Section 22589.11.

(b) If a social media company uses an open protocol that the Attorney General identifies under subdivision (a), the social media company shall be entitled to a rebuttable presumption that the social media company provides access on reasonable terms that do not discriminate.

22589.15. (a) The Attorney General shall enforce this chapter.

(b) A social media company or ~~model operator~~ ***deployer*** that violates this chapter shall be liable for an administrative fine of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation.

(c) In a proceeding brought pursuant to this chapter, the Attorney General may petition for appropriate injunctive relief.

ARGUMENTS IN SUPPORT: Project Liberty, sponsor of the bill, writes in support:

Today, the internet too often strips individuals of their agency. Social media and AI companies hoard personal data, manipulate algorithms for profit, and design systems that trap users—especially children—in environments that fuel anxiety, misinformation, and exploitation.

Families have little power to protect their children's well-being or move their information to safer, healthier digital spaces. The Digital Choice Act offers a path forward by enshrining two essential rights:

● Portability: the ability to download and move your data, content, and interactions in a usable format;

● Interoperability: the freedom to connect across platforms, ending corporate control over our digital relationships.

These solutions are not just theoretical—they are technologically feasible and in place today. Project Liberty's open protocol, the Decentralized Social Networking Protocol (DSNP), is one example of an open protocol that implements full data portability and interoperability at scale today. Much like the open standards that make email or the web function seamlessly, DSNP allows individuals to control access to their own data across platforms. Millions of people are already using interoperable social networks built on DSNP and similar technologies, proving this model is both practical and safe.

In fact, platforms should already be preparing for a future of interoperability. A law in Utah requiring comparable interoperability and data portability functionality will take effect on July 1, 2026, following an implementation period. By acting now, California can lead in protecting its residents' rights, without creating additional technical burdens.

This bill strengthens individual agency and creates a foundation for innovation. It encourages platforms to compete on safety, transparency, and wellbeing — not just engagement and profit. For children and families, this means digital environments that nurture connection and creativity, not addiction or harm.

The Digital Choice Act will also strengthen privacy and security by putting individuals—not corporations—in control of their data. Under today's centralized systems, social media and AI companies store, mine, and sell users' personal information, creating vast repositories that are prime targets for hackers. By giving people ownership of their own data and the ability to decide if, when, and how it is shared, the Act limits unnecessary exposure and third-party harvesting.

Instead of concentrating sensitive information in a few corporate servers, a decentralized and interoperable system disperses risk and protects against mass breaches. Existing open protocols, such as DSNP, also already support end-to-end encryption, so individuals can communicate and share safely while maintaining privacy and control. The Digital Choice Act would require platforms to protect individuals' data privacy and security in implementing its provision, ensuring they select privacy-protecting technologies while maintaining flexibility.

Also writing in support, a coalition of technology organizations, including Tech Equity and Tech Oversight argues:

> A growing body of evidence shows that social media and AI platforms can cause significant harm, yet users often feel unable to leave. A nationally representative 2024 survey of Gen Z adults found that 40% wish many forms of social media had never been invented, even as 60% report using it for four or more hours daily and say it negatively affects their lives. Emerging research on AI systems reveals similar patterns, with users reporting dependency, withdrawal-like symptoms, and emotional over-attachment to AI companions. (See e.g., Harris Poll and ScienceDirect.)

Recent litigation underscores these risks. In 2026, Google and Character.AI agreed to settle multiple lawsuits alleging harms to minors, including wrongful death claims tied to chatbot interactions. (See CNBC) These cases highlight the real-world consequences of highly engaging systems that lack sufficient safeguards.

Despite these harms, users remain locked into platforms due to structural barriers. Research shows that individuals are far more willing to leave platforms if their peers do so as well, illustrating the power of network effects. Other studies estimate that a substantial share of a platform's value comes from users' existing social networks—connections that are lost when switching services. AI systems are now reinforcing these dynamics by storing user preferences and histories in non-transferable formats, further increasing switching costs.

Experience from other sectors demonstrates that portability and interoperability can effectively reduce these barriers. Open banking reforms across dozens of countries have led to increased startup formation, investment, and consumer choice. Similarly, number portability in telecommunications reduced prices and improved competition by lowering switching costs.

Leading experts and regulators, including the Federal Trade Commission, have identified interoperability as a key tool to address platform lock-in. Current voluntary data portability measures are insufficient. Platforms typically provide only limited exports of user-submitted data, excluding the inferred and relational data that drive personalization. As a result, users cannot meaningfully transfer their digital lives to competing services. Importantly, portability is not theoretical. Platforms built on interoperable protocols with tens of millions of users already allow users to move their identity, content, and connections across services without disruption—demonstrating that a more competitive and user-centered digital ecosystem is achievable.

ARGUMENTS IN OPPOSITION: In opposition to the bill, a coalition of business organizations that is led by the Computer and Communications Industry Association and includes TechNet and the California Chamber of Commerce raises the following concerns (in addition to those previously discussed in the analysis):

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). By granting the Attorney General the power to "assess" and "identify" which protocols are acceptable, the state creates a permissioned 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. 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.

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, 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. 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.

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." 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." 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.

REGISTERED SUPPORT / OPPOSITION:

Support

Project Liberty LLC (Sponsor)
18 Individuals
Anxious Generation Foundation
California Initiative for Technology and Democracy (CITED)
Children Now
Children's Advocacy Institute, University of San Diego School of Law
Epic
Kapor Center Advocacy
Mothers Against Media Addiction
Oakland Privacy
Privacy Rights Clearinghouse
Radicalxchange Foundation
Tech Oversight Project Dba Tech Oversight California
TechEquity Action
Transparency Coalition.ai

Opposition

California Chamber of Commerce
Chamber of Progress
Civil Justice Association of California (CJAC)
Computer & Communications Industry Association
Insights Association
Software Information Industry Association
Technet

Oppose Unless Amended

Calbroadband

Analysis Prepared by: Julie Salley / P. & C.P. / (916) 319-2200