



March 26, 2024

Assembly Committee on Privacy and Consumer Protection
Room 162, Legislative Office Building
1020 N Street
Sacramento, CA 95814

RE: AB 2461, “Social Media User Authentication” (Oppose)

Dear Chair Bauer-Kahan and Members of the Assembly Committee on Privacy and Consumer Protection:

The seven co-signed organizations have serious concerns about mandating user authentication mechanisms on social media platforms. Specifically, the bill would require social media companies to develop a mechanism to collect, maintain, and authenticate sensitive personal information. Various online and digital services may choose to employ a variety of different tools and features, which may not rely on collecting a user’s state identification. Certain tools and features support protecting the identity or anonymity of their users, and businesses aim to tailor these appropriately to the nature of the service and online community the service is trying to create and foster.

However, mandating such a requirement would impede social media platforms’ ability to make those decisions, in turn impacting the service and community they offer. For example, certain social media platforms may choose to implement optional user authentication in response to malicious actors or spam bot accounts. By forcing all social media platforms to implement user

authentication, this in turn would require companies to collect sensitive information. Many social media platforms do not want to collect such information as they could be held liable for potential data breaches.

Alternatively, a social media platform could choose *not* to offer user authentication due to concerns that users are not comfortable sharing certain personal information, for example, if they are speaking about a sensitive topic or are from a vulnerable community. Many users opt to use pseudonyms or no name at all when engaging in online speech. Anonymous speech is a long-held value and tradition in the United States, dating back to the Federalist Papers, famously penned under “Publius” and “Federal Farmer”. Protecting anonymity of online speech carries forward such traditions and protections to allow for open and free expression. By mandating that an online community be bifurcated into “authenticated” and “non-authenticated” users, it risks disincentivizing online anonymity lest “non-authenticated” accounts be viewed as less safe or legitimate.

Currently, many social media platforms do choose to offer such optional user authentication, such as on online dating websites to allow users to have more assurance that a person they may choose to meet in-person is being honest about who they are. However, this is an independent choice of the specific service to address a certain context. Other social media platforms offer authentication but require users to pay a fee. It should be noted that implementing any user authentication mechanism requires a significant amount of resources. Social media platforms would need to build the features into their current model and ensure that appropriate data security measures are in place due to the exchange of personal information, such as valid state identification, as required under AB 2461. This could create a chilling effect upon users as it risks having additional data stolen or linked to a user’s social media account.

Finally, it is unclear how requiring social media platforms to implement an optional user authentication model would provide any benefit for users and it could create a false sense of security. Bad actors could exploit such mechanisms, particularly if they hack and take over a verified user’s account. The hacked verified account could be used to help spread misinformation or damage the user’s reputation. And other users might not be aware of the account compromise but assume that the account is safe to engage with and trustworthy just because it is labeled as “authenticated”. Because AB 2461 would require a user to submit a valid state identification, bad actors could easily focus efforts on spoofing and creating fake state IDs. In effect, this would allow such actors to bypass a myriad of other security mechanisms used by different platforms.

* * * * *

For the above reasons, we urge you to resist advancing legislation that imposes burdensome requirements on social media platforms with little to no benefit to users.

Respectfully submitted,

Khara Boender, Computer & Communications Industry Association (CCIA)

Ronak Daylami, California Chamber of Commerce (CalChamber)

Todd O'Boyle, Chamber of Progress

Carl Szabo, NetChoice

Shoshana Weissman, R Street Institute

Anton Van Seventer, Software & Information Industry Association (SIIA)

Dylan Hoffman, TechNet

CC: Assemblymember Devon Mathis
Suite 5530, State Capitol
1021 O Street
Sacramento, CA 95814