April 3, 2024

Senate Committee on Judiciary
1021 O Street, Room 3240
Sacramento, CA 95814

RE: SB 1228, "Large online platforms: user identity authentication" (Oppose)

Dear Chair Umberg and Members of the Senate Committee on Judiciary:

The above seven co-signed organizations have serious concerns about mandating user authentication mechanisms on "large online platforms". Specifically, SB 1228 would require a "large online platform" to "seek to verify an influential user's name, telephone number, and email address" by a means of the large online platform's choosing. SB 1228 further requires a large online platform to verify a "highly influential user" by reviewing a government-issued identification. These requirements could negatively impact users' ability to freely communicate online, particularly when engaged in anonymous speech, and raise security and privacy concerns.

We appreciate the opportunity to expand on the issues raised under the proposed provisions in SB 1228.

Definitions under SB 1228 raise significant questions surrounding compliance.

SB 1228's definition of "highly influential user" would include users whose authored, created, or shared content "has been seen by more than 25,000 users over the lifetime of the accounts that they control or administer on the platform". This threshold could be easily met due to the abundance of bot accounts and bot farms, thus mandating user authentication effectively by default for a large number of users.

Covered platforms would likely face several difficult scenarios when attempting to come into compliance with SB 1228's provisions. For example, it is unclear how a covered platform would need to address existing verified users on the platform, especially if, for example, the initial verification was conducted using a method that does not rely on the use of government-issued identification. Covered platforms would need to know whether re-authenticating the user would be necessary, which could create user frustration if they are unwilling to provide such personal information.

Additional clarity is also needed to understand how a covered platform should treat a user who is considered "highly influential" on another platform, but may not have met similar threshold requirements on their own service. Therefore, covered platforms would need to understand how SB 1228's definitions would apply across various online services.

Mandatory online user authentication requirements would impede covered platforms' ability to choose whether that is appropriate for their service.

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. Currently, many online 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. For example, other online services may choose to implement optional user authentication in response to malicious actors or spam bot accounts.

There are many reasons online platforms and users may choose to preserve online anonymity.

An online 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. SB 1228 raises the likelihood of this effect because the bill would require "large online platforms" to show, for at least two seconds prior to the rest of the post being available, a message akin to "this user is unauthenticated" for any user that has not complied with the platform's authentication process. This could appear to serve as a "red flag" or warning for other users for any unauthenticated user's content.

User authentication requires additional data collection and could create security risks.

By forcing all large online platforms to implement various levels of user authentication, this in turn would require companies to collect sensitive information. It should be noted that implementing any user authentication mechanism requires a significant amount of resources. Online 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 government-issued identification, as required under SB 1228 for "highly influential users". This could create a chilling effect upon users as it risks having additional data stolen or linked to a user's social media account.

Many online platforms do not want to collect additional information associated with authentication as they could be held liable for potential data breaches. SB 1228 makes it clear that a covered platform must protect a user's information and "not allow a user's sensitive personal information to become public." It is unclear whether covered platforms would face liability if this collected sensitive personal information is disclosed via a breach. While such platforms may implement strong, industry-standard security measures, nefarious actors are constantly evolving and advancing new tactics to circumvent existing protective frameworks. Governments and private businesses alike are subject to security risks on a daily basis and mandating the additional collection of sensitive information only heightens this risk. Because the explicit requirement to provide a government-issued identification is limited to the most influential users, it creates a known and particularly appealing honeypot of information for bad actors to potentially exploit.

It is unclear how requiring online platforms to implement the prescribed user authentication model under SB 1228 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 SB 1228 would require “highly influential users” to submit a government-issued 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 online 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
Jasson Crocket, Snap Inc.
Paul Lekas, Software & Information Industry Association (SIIA)
Dylan Hoffman, TechNet

CC: Senator Steve Padilla
Suite 6640, State Capitol
1021 O Street
Sacramento, CA 95814-4900