SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2023-2024 Regular Session

SB 1228 (Padilla)
Version: April 10, 2024
Hearing Date: April 23, 2024
Fiscal: Yes
Urgency: No
CK

SUBJECT

Large online platforms: user identity authentication

DIGEST

This bill requires large online platforms to seek to verify influential users, as provided, and to label such accounts and their posts with notes that the user is or is not authenticated by the platform. The bill authorizes public prosecutors to file prioritized actions to enjoin violations and seek other equitable relief.

EXECUTIVE SUMMARY

Democracy and truth are under assault on a daily basis in this country. Political polarization and distrust in not only government, but the electoral process, are fueled by misinformation and disinformation, both coordinated and not. The impacts of false news are widespread, poisoning public discourse and deliberative processes, undermining our institutions, and shattering any sense of joint reality.

The overwhelming battleground for this assault is on social media platforms. Recent surveys estimate that half of adults in the United States get at least some of their news from social media. In fact, three in ten Americans say they regularly get news on Facebook. With the threat of coordinated hostile government campaigns and massive bot armies, it can be difficult to sort through the noise. This bill seeks to provide some level of transparency on these platforms by requiring platforms to at least seek to verify the identity of their most influential users. If they are successful, they are required to mark such accounts and their posts with an authenticated tag. If they are not, then the tag labels the content and accounts as unauthenticated.

This bill is sponsored by California Initiative for Technology and Democracy (CITED). It is supported by several advocacy groups, including the Asian Law Alliance. It is opposed by a coalition of industry associations, including Technet and Snap, Inc.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Requires social media platforms to semiannually report a detailed description of its content moderation practices including information on its policies to address disinformation or misinformation and details on how much content was flagged as such and what the platform did in response. (Bus. & Prof. Code § 22677.)

2) Provides that proceedings in cases involving the registration or denial of registration of voters, the certification or denial of certification of candidates, the certification or denial of certification of ballot measures, election contests, actions under Chapter 2 (commencing with Section 21100) of Division 21 of the Elections Code, and actions under Chapter 22.9 (commencing with Section 22684) of Division 8 of the Business and Professions Code, shall be placed on the calendar in the order of their date of filing and shall be given precedence. (Code Civ. Proc. § 35.)

This bill:

1) Requires a large online platform to seek to verify the following:
    - An influential user's name, telephone number, and email address by a means chosen by the large online platform.
    - A highly influential user's identity by asking to review the highly influential user's government-issued identification.

2) Requires a large online platform to protect any identification information provided by an influential user in compliance with this section using, at a minimum, the standard of the industry used to protect the confidential information of users unless the platform makes that information public in the normal course. However, a large online platform shall not allow a user's sensitive personal information to become public and none of the identification information can be used for any purpose other than compliance with this bill. A large online platform shall maintain proof that it has complied with the verification requirements of this section but may refrain from storing or maintaining the verification information or documentation.

3) Requires a large online platform to note on the profile page of an influential or highly influential user, in type at least as large and as visible as the user's name, either of the following:
    - "This user has been authenticated," or some similar phrase, if the user has complied with the identification process.
    - "This user is unauthenticated," or some similar phrase, if the user has failed to comply.

4) Requires the platform to attach to any post of an influential or highly influential user a notation that would be understood by a reasonable person as indicating that the user is authenticated or unauthenticated. If unauthenticated, the notation shall be visible for at least two seconds before the rest of the post is visible and remain with the post thereafter.

5) Provides that a large online platform shall allow its users to opt out of receiving any posts, information, or other distributions from a user who is not authenticated.

6) Defines the relevant terms, including:
    - "Highly influential user" means a user of a large online platform that meets any of the following criteria:
        - Content authored, created, or produced by the user has been seen by more than 100,000 users within a seven-day period over all of the accounts that they control or administer on the platform.
        - Accounts controlled or administered by the user have more than 30,000 followers.
        - The user ranks in the top 3 percent of users by amount of content viewed by users on the platform within a seven-day period over all of the accounts that the user controls or administers on the platform.
    - "Influential user" means a user of a large online platform that meets any of the following criteria:
        - Content authored, created, or produced by the user has been seen by more than 50,000 users within a seven-day period over all of the accounts that the user controls or administers on the platform.
        - Accounts controlled or administered by the user have more than 15,000 followers.
        - The user ranks in the top 6 percent of users by amount of content viewed by users on the platform within a seven-day period over all of the accounts that the user controls or administers on the platform.
    - "Large online platform" means a public-facing website, web application, or digital application, including a social network, video sharing platform, messaging platform, advertising network, or search engine that had at least 1,000,000 California users during the preceding 12 months.

7) Authorizes the Attorney General or any district attorney or city attorney to file an action to seek injunctive or other equitable relief against a large online platform to compel compliance. The court is required to award a prevailing plaintiff reasonable attorney's fees and costs.

8) Clarifies that it does not preclude a large online platform from more stringent identification verification procedures.

9) Clarifies that it does not require a large online platform to provide less exposure or visibility to the posts made or digital media content created by users who decline to provide identity verification.

10) Includes a severability clause.

11) Prioritizes civil actions brought for violations.

COMMENTS

1. Social media and the rise of misinformation and disinformation

In 2005, five percent of adults in the United States used social media. In just six years, that number jumped to half of all Americans. Today, over 70 percent of adults use at least one social media platform. Facebook alone is used by 69 percent of adults, and 70 percent of those adults say they use the platform on a daily basis. As stated, half of Americans rely on social media for at least some of their news leading to the conclusion: "Digital news has become an important part of Americans' news media diets, with social media playing a crucial role in news consumption."[1]

Given the reach of social media platforms and the role they play in many people's lives, concerns have arisen over what content permeates these sites, entering the lives of the billions of users, and the effects it has on them and society as a whole. In particular, the sharpest calls for action focus on the rampant spread of misinformation and disinformation and the effects it has on our political discourse and faith in democracy and its institutions. According to the Brookings Institution:

> [A] Quinnipiac University survey reveals that 76% of respondents think political instability within the country is a bigger danger to the United States than external adversaries. Amazingly, this suggests that Americans recognize that we are a bigger threat to our own democracy than any other potential external threat. Sadly, according to this poll, over half of Americans (53%) expect political divisions in the country to worsen over their lifetime rather than get better.

[1] *Social Media and News Fact Sheet* (November 15, 2023) Pew Research Center, https://www.pewresearch.org/journalism/fact-sheet/social-media-and-news-fact-sheet/. All internet citations are current as of April 15, 2024.

> One of the drivers of decreased confidence in the political system has been the explosion of misinformation deliberately aimed at disrupting the democratic process. This confuses and overwhelms voters.[2]

The 2016 election was a major breaking point for many. Investigations uncovered attempted interference in the United States Presidential election through a social media "information warfare campaign designed to spread disinformation and societal division in the United States."[3] The United States Senate Select Committee on Intelligence issued a report detailing how Russian operatives carried out their plan:

> Masquerading as Americans, these operatives used targeted advertisements, intentionally falsified news articles, self-generated content, and social media platform tools to interact with and attempt to deceive tens of millions of social media users in the United States. This campaign sought to polarize Americans on the basis of societal, ideological, and racial differences, provoked real world events, and was part of a foreign government's covert support of Russia's favored candidate in the U.S. presidential election.

This again became a threat in the 2020 election, with social media rife with misinformation such as the incorrect election date,[4] and then social media became a hotbed of misinformation about the results of the election.[5] The author points to investigations that have found the violent insurrectionists that stormed the Capitol on January 6, 2021, were abetted and encouraged by posts on social media sites.[6] In response to indications that social media provided a venue for those who overran and assaulted police officers, Facebook deflected blame, asserting that "these events were largely organized on platforms that don't have our abilities to stop hate, don't have our

---

[2] Gabriel R. Sanchez & Keesha Middlemass, *Misinformation is eroding the public's confidence in democracy* (July 26, 2022) Brookings Institution, https://www.brookings.edu/articles/misinformation-is-eroding-the-publics-confidence-in-democracy/.

[3] Select Committee on Intelligence, Russian Active Measures, Campaigns, and Interference in the 2016 U.S. Election, United States Senate, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

[4] Pam Fessler, *Robocalls, Rumors And Emails: Last-Minute Election Disinformation Floods Voters*, NPR (October 24, 2020), https://www.npr.org/2020/10/24/927300432/robocalls-rumors-and-emails-last-minute-election-disinformation-floods-voters.

[5] Sheera Frenkel, *How Misinformation 'Superspreaders' Seed False Election Theories*, New York Times (November 23, 2020), https://www.nytimes.com/2020/11/23/technology/election-misinformation-facebook-twitter.html; Philip Bump, *The chain between Trump's misinformation and violent anger remains unbroken*, Washington Post (May 12, 2021), https://www.washingtonpost.com/politics/2021/05/12/chain-between-trumps-misinformation-violent-anger-remains-unbroken/.

[6] Ken Dilanian & Ben Collins, *There are hundreds of posts about plans to attack the Capitol. Why hasn't this evidence been used in court?* (April 20, 2021) NBC News, https://www.nbcnews.com/politics/justice-department/we-found-hundreds-posts-about-plans-attack-capitol-why-aren-n1264291.

standards, and don't have our transparency."[7] However, later indictments of those perpetrating the attack "made it clear just how large a part Facebook had played, both in spreading misinformation about election fraud to fueling anger among the Jan. 6 protesters, and in aiding the extremist militia's communication ahead of the riots."[8] Three in ten Americans regularly get their news from Facebook.[9]

2. A measure of transparency on social media

According to the author:

> Foreign adversaries hope to harness new and powerful technology to misinform and divide America this election cycle. Bad actors and foreign bots now have the ability to create fake videos and images and spread lies to millions at the touch of a button. We need to ensure our content platforms protect against the kind of malicious interference that we know is possible. Verifying the identities of accounts with large followings allows us to weed out those that seek to corrupt our information stream.

This bill attempts to tackle the problem by providing more transparency about who is behind the most influential social media accounts. The bill creates two tiers of users with wide reach:

- "Highly influential user" means a user of a large online platform that meets any of the following criteria:
    - Content authored, created, or produced by the user has been seen by more than 100,000 users within a seven-day period over all of the accounts that they control or administer on the platform.
    - Accounts controlled or administered by the user have more than 30,000 followers.
    - The user ranks in the top 3 percent of users by amount of content viewed by users on the platform within a seven-day period over all of the accounts that the user controls or administers on the platform.
- "Influential user" means a user of a large online platform that meets any of the following criteria:
    - Content authored, created, or produced by the user has been seen by more than 50,000 users within a seven-day period over all of the accounts that the user controls or administers on the platform.

---

[7] Sheera Frenkel & Cecilia Kang, *Mark Zuckerberg and Sheryl Sandberg's Partnership Did Not Survive Trump* (July 8, 2021) The New York Times, https://www.nytimes.com/2021/07/08/business/mark-zuckerberg-sheryl-sandberg-facebook.html.
[8] *Ibid.*
[9] *See* fn. 1.

- Accounts controlled or administered by the user have more than 15,000 followers.
- The user ranks in the top 6 percent of users by amount of content viewed by users on the platform within a seven-day period over all of the accounts that the user controls or administers on the platform.

The bill requires platforms to seek to verify the identity of these influential and highly influential users. For the first tier, the platform must seek to verify the user's name, telephone number, and email address by whatever means they choose. For the higher threshold, platforms must seek to verify highly influential user's identity by asking to review their government-issued identification.

Based on whether or not that process is successful, the platform must place a label on both the user's profile and on their posted content that notes whether the user is authenticated or unauthenticated, although it is not prescriptive about the phrasing.

The California Initiative for Technology & Democracy (CITED), the sponsor of this bill, write:

> California and the nation are entering an election season in which disinformation will pollute our information ecosystems like never before. In just a few clicks and at little-to-no cost, anyone has the power to create increasingly realistic deceptive content and then spread that fake digital media to millions very quickly over online platforms. Therefore, we need to have strong protections in place at the points of scaled dissemination. Examples of this occurring in U.S. elections include Ron Desantis using AI-generated images to attack his opponent in his presidential run, coordinated foreign actors caught attempting to influence American politics through social media, and just this month, a supporter of former President Trump created a deepfake image of Trump designed to influence Black voters.
>
> Social media users with the largest reach, including influencers and bot accounts acting in a coordinated manner to amplify discourse, have an outsized ability to amplify disinformation quickly. Furthermore, while some social media accounts accurately convey the individual behind the account, many usernames and profiles do not disclose any personal identifying information, and may even seek to mislead others as to the true identity behind the account. While anonymity can be useful in some contexts, such as allowing political dissidents to speak their mind without fear of repercussion, studies suggest more broadly that anonymity online is leading to manipulation and unaccountable communication.

> Studies have found that anonymity online results in reduced inhibition and personal responsibility, and is associated with a lack of accountability, increased "unconstrained posting," and increased aggressiveness.
> Additional academic research highlights that, particularly on social media in which sources of content tend to look the same, users have difficulty assessing the source's credibility, and lack the context needed to accurately judge the interests, agendas, or biases of the source of information. Voters simply do not know what images, audio, and video they can trust, or which users to believe.
>
> Fortunately, California need not look far for solutions. Other industries, like banking, lending, and credit card companies, are required to employ "Know Your Customer" principles before allowing people to use their services. Under these principles, companies take steps to verify customer identities and to protect against fraud, corruption, and illegal activity. Higher levels of information may be required for customers that are identified as higher risk, allowing financial institutions to develop an understanding of the customer's typical behavior in order to quickly identify suspicious activity.
>
> Applying these same principles to social media accounts can help mitigate and slow the spread of disinformation. Escalating identity verification requirements on users may also impact the behavior of the users themselves as well as the viewers. Labeling is a time-tested method for providing consumers and voters more relevant information for their decision-making process, but has also been shown to impact the behavior of those subject to the labels.

A coalition of tech companies and industry associations, including the Computer and Communications Industry Association writes in opposition:

> **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.

As to the privacy concerns, the bill has several mechanisms to mitigate the impact. First, it requires platforms to protect this information and to never allow sensitive personal information from becoming public. The bill also strictly limits what the platform can use this information for: only compliance with its provisions. In fact, while platforms are required to maintain proof of their own compliance with the law, they are not

required to store or maintain the verification information or documentation. In response to the concerns about the bill's impact on speech, CITED states:

> Importantly, this bill balances free speech objectives with appropriate disclosures to the public related to users and their content. It does not silence or censor users and it passes no subjective judgment on the content. It simply makes it clear whether the person posting the information is a verified person or not. And because it only mandates the request of identity information from the users with the very largest audiences, it changes nothing about the user experience for the vast majority of social media users.

The bill is subject to only public enforcement and provides for only injunctive and other equitable relief as well as attorney's fees and costs. The bill provides that such actions will be calendared in the order of their date of filing and given precedence over other cases. This latter provision would have such actions jump in front of many other very worthy matters. The author has agreed to remove this provision.

In addition, in order to ensure there is consistency in the law, the author has agreed to amendments that utilize the existing definition for social media platform found in Business and Professions Code section 22675, but will continue to limit it to social media platforms with at least one million California users during the preceding 12 months.

SUPPORT

California Initiative for Technology & Democracy (sponsor)
AFSCME, AFL-CIO
Asian Law Alliance
Bay Rising
California Clean Money Campaign
Chinese Progressive Association
Courage California
Hmong Innovating Politics
Partnership for the Advancement of New Americans
SEIU California

OPPOSITION

California Chamber of Commerce
Chamber of Progress
Computer and Communications Industry Association
Internet.works
Netchoice

Oakland Privacy
SNAP Inc.
Software & Information Industry Association
Technet

RELATED LEGISLATION

Pending Legislation: AB 2839 (Pellerin, 2024) prohibits a person, committee, or other entity from knowingly distributing an advertisement or other election communication, as defined, that contains certain materially deceptive and digitally altered or digitally created images or audio or video files, as defined, with the intent to influence an election or solicit funds for a candidate or campaign, subject to specified exemptions. AB 2839 is currently on the Assembly Floor.

Prior Legislation: AB 587 (Gabriel, Ch. 269, Stats. 2022) required, among other things, social media platforms to semiannually report a detailed description of its content moderation practices including information on its policies to address disinformation or misinformation and details on how much content was flagged as such and what the platform did in response.

****