Date of Hearing: April 30, 2024

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 2461 (Mathis) – As Amended April 9, 2024

AS PROPOSED TO BE AMENDED

SUBJECT: User authentication

SYNOPSIS

There are a number of bills currently moving through the legislature that require users of various platforms to either submit personal information to prove they are who they say they are or to verify their age in order to access certain sites on the internet, such as pornography sites. The policy efforts of both protecting children online and working to slow misinformation by requiring that the social media accounts of identifiable individuals be verified are arguably laudable goals. However, requiring someone to submit personal information, including banking information or an official government identification, raises significant concerns among privacy experts. Each additional piece of information can be monetized by either selling it to data brokers who create extensive dossiers on individual internet users that they then sell to others or by being compiled by the platform itself to develop detailed information that can be used to target advertising and content at users.

Requiring social media platforms to implement various types of user authentication would likely result in companies collecting more sensitive personal information. While online platforms may argue that they do not want to be forced to collect more information from users, given that the operators of social media platforms primarily earn their revenue through digital advertising to their users and by keeping people attached to their platforms, these companies have a strong financial incentive to design their products to maximize the time users spend on their social media. The collection and exploitation of personal information is in large part what enables businesses to harness the algorithmic delivery of content designed to lead to social media addiction in children, and drive up company profits in the process. Given that, it is unlikely that platforms are reluctant to gather more personal information on their users.

This bill seeks to find that balance by allowing for personal information to be collected for verification purposes, but also strictly limits the length of time the data can be kept and the ways in which it can be used. Any efforts to retain, sell, or share the data will be strictly prohibited.

The suggested Committee amendments clarify the restrictions placed on the personal information collected for verification purposes, including strictly prohibiting its use for anything other than the intended purpose. In addition, the amendments shorten the data retention time for personal information that is collected for the purpose of user verification from 30 days to 48 hours. Once the verification process is completed, it is unclear why a social media platform would need to retain the personal information collected. Restricting the use of the personal information and limiting the data retention period are both in keeping with the state's data minimization goals.

SUMMARY: Requires a social media platform that authenticates the identity of a user to delete any personal information submitted by the user for purposes of authentication within 48 hours after the authentication is completed. Specifically, **this bill**:

1) Requires social media platforms, as defined, to delete within 48 hours of completing an authentication process, all personal information submitted by the user to the platform for the purpose of authenticating the user's identity or age.

2) Prohibits a social media platform from using the identification information provided by a user for the purpose of complying with the bill's provisions for any purpose other than authenticating the user's identity or age.

3) Requires a social media platform to protect any identification information provided by a user in compliance with this section using, at a minimum, the standard of the industry used to protect the confidential information of users.

4) Authorizes the Attorney General or any district attorney, county counsel or city attorney may seek injunctive or other equitable relief against a large online platform to compel compliance with this chapter. Requires, in such actions, the court to award a prevailing plaintiff reasonable attorney's fees and costs.

5) Defines a "social media platform" as a public or semi-public internet-based service or application that has users in California and a substantial function of the service is to connect users in order to allow them to interact socially over the platform. In addition, the platform allows users to construct a profile, populate a list of users with whom they share a social connection, and create or post content viewable by other users.

6) Defines a "user" as a natural person who is a resident of California and has an active account with a social media platform.

7) States that "personal information" and "sensitive personal information" has the same meaning as defined in the California Consumer Privacy Act (CCPA).

EXISTING LAW:

1) Provides, pursuant to the California Constitution, that all people are by nature free and independent and have inalienable rights. Among these the fundamental right to privacy. (Cal. Const. art. I, § 1.)

2) Establishes the California Consumer Privacy Act. (Civ. Code §§ 1798.100-1798.199.100.)

3) Limits a business' collection, use, retention, and sharing of a consumer's personal information to that which is reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes. (Civ. Code § 1798.100(c).)

4) Requires sellers of products or services that are illegal to sell to minors to take reasonable steps to ensure that the purchaser is of legal age at the time of the purchase or delivery, including but not limited to verifying the age of the purchaser. (Civ. Code § 1798.99.1(a).)

5) Provides that reasonable steps include:

   a) The provision of a government-issued identification, subject to all laws governing retention, use, and disclosure of personally identifiable information,

   b) Requiring the purchaser to use a nonprepaid credit card for an online purchase, or

   c) Implementing a system that restricts individuals with accounts designated as minor accounts from purchasing the prohibited products. (Civ. Code § 1798.99.1(a)(2).)

6) Prohibits a person or business subject to 4) from retaining, using, or disclosing any information it receives from a purchaser or recipient in an effort to verify age for any purpose other than as required by law. (Civ. Code § 1798.99.1(a)(6).)

7) Defines the following terms under the CCPA:

   a) "Personal information" means 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. Personal information includes such information as:

      i) Name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other identifier.

      ii) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

      iii) Biometric information.

      iv) Internet activity information, including browsing history and search history.

      v) Geolocation data.

      vi) Audio, electronic, visual, thermal, olfactory, or similar information.

      vii) Professional or employment-related information. (Civ. Code § 1798.140(v).)

   b) "Sensitive personal information" means personal information that reveals a person's:

      i) Social security, driver's license, state identification card, or passport number.

      ii) Account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials.

      iii) Precise geolocation.

iv) Racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership.

v) Email, mail and text messages.

vi) Genetic data.

vii) Information collected and analyzed relating to health.

viii) Information concerning sex life or sexual orientation. (Civ. Code § 1798.140(ae).)

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

a) A substantial function of the service or application is to connect users in order to allow them to interact socially with each other within the service or application. (A service or application that provides email or direct messaging services does not meet this criterion based solely on that function.)

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 § 22945(a)(3).)

FISCAL EFFECT: As currently in print, this bill is keyed non-fiscal.

COMMENTS:

1) **Balancing the need to protect privacy with the need to verify the authenticity of users and their ages.** There are a number of bills currently moving through the legislature that require users of various platforms to either submit personal information to prove they are who they say they are or to verify their age in order to access certain sites on the internet, such a pornography sites. The policy efforts of both protecting children online and working to slow misinformation by requiring that the social media accounts of identifiable individuals be verified are arguably laudable goals. However, requiring someone to submit personal information, including banking information or an official government identification, raises significant concerns among privacy experts. Each additional piece of information can be monetized by either selling it to data brokers who create extensive dossiers on individual internet users that they then sell to others or by being compiled by the platform itself to develop detailed information that can be used to target advertising and content at users.

Requiring social media platforms to implement various types of user authentication would likely result in companies collecting more sensitive personal information. While online platforms may argue that they do not want to be forced to collect more information from users, given that the

operators of social media platforms primarily earn their revenue through digital advertising to their users and by keeping people attached to their platforms, these companies have a strong financial incentive to design their products to maximize the time users spend on their social media. The collection and exploitation of personal information is in large part what enables businesses to harness the algorithmic delivery of content designed to lead to social media addiction in children, and drive up company profits in the process. Given that, it is unlikely that platforms are reluctant to gather more personal information on their users. This bill seeks to find that balance by allowing for personal information to be collected for verification purposes, but also strictly limits the length of time the data can be kept and the ways in which it can be used. Any efforts to retain, sell, or share the data will be strictly prohibited.

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

> In the current digital age and with increasing cyber-attacks against technology companies, it is paramount that we take active steps to protect the privacy of online users. AB 2461 will protect user data by ensuring that social media platforms who receive our identification for the purposes of user authentication are required to delete their users' identity information within a timely manner.

3) **Surveillance capitalism.** For almost 20 years experts have been warning us about the erosion of our private lives. They note that this erosion is happening one small bit at a time, likely without people even noticing. With the advent of the internet and advances in technology, it is no longer easy for people to decide which aspects of their lives should be publicly disclosed. As Alex Preston noted in *The Guardian* a decade ago:

> We have come to the end of privacy; our private lives, as our grandparents would have recognised them, have been winnowed away to the realm of the shameful and secret. . . . Insidiously, through small concessions that only mounted up over time, we have signed away rights and privileges that other generations fought for, undermining the very cornerstones of our personalities in the process. While outposts of civilisation fight pyrrhic battles, unplugging themselves from the web. . . the rest of us have come to accept that the majority of our social, financial and even sexual interactions take place over the internet and that someone, somewhere, whether state, press or corporation, is watching.[1]

Since the time this piece was published, it has become increasingly clear that not only is our right to privacy significantly eroded, but our private information and activities are now being harvested and sold for a profit. This commodification of personal information has been dubbed "surveillance capitalism" by social psychologist, Shoshana Zuboff. In an opinion piece for *The New York Times*, in 2021, Dr. Zuboff warned:

> As we move into the third decade of the 21st century, surveillance capitalism is the dominant economic institution of our time. In the absence of countervailing law, this system successfully mediates nearly every aspect of human engagement with digital information. The promise of the surveillance dividend now draws surveillance economics into the "normal" economy, from insurance, retail, banking and finance to agriculture, automobiles, education, health care and more. . . .

---

[1] Preston, Alex. "The death of privacy." *The Guardian* (Aug. 3, 2014) *available at* https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston.

> An economic order founded on the secret massive-scale extraction of human data assumes the destruction of privacy as a nonnegotiable condition of its business operations. With privacy out of the way, ill-gotten human data are concentrated within private corporations, where they are claimed as corporate assets to be deployed at will.[2]

Some may consider sharing their private information, including websites they visit, purchases, employment history, menstrual cycles, name, pictures, locations and movements, social media posts and reactions, and other seemingly innocuous information a reasonable price to pay for freely accessing the internet. However, not protecting that personal information can have real world consequences. As an example, dating app, Grindr, was fined 10 percent of its global annual revenue by the Norwegian Data Protection Authority in 2021 for sharing deeply personal information with advertisers, including location, sexual orientation and mental health details.[3] This was not the first time Grindr had failed to protect their users' private information. Several years earlier, it was revealed that the company had shared HIV status and the location data from their users with two companies who were contracted to optimize the Grindr platform.[4]

This slow erosion of privacy, through the collection of relatively small pieces of personal information may not cause people to be overly concerned. However, the private information being amassed on everyone in the United States that is being made available to individuals, private companies, and local, state, and federal government agencies should alarm everyone. University of Virginia Law Professor, Danielle Citron, warned in an interview with The Guardian in 2022, "We don't viscerally appreciate the ways in which companies and governments surveil our lives by amassing intimate information about our bodies, our health, our closest relationships, our sexual activities and our innermost thoughts. Companies are selling this information to data brokers, who are compiling dossiers with about 3,000 data points on each of us."[5]

Catherine Powell pointed out in 2023 in a blog post for the *Council on Foreign Affairs*:

> If you've engaged with any form of technology recently—whether through a smartphone, social media, a fitness tracker, even a seemingly innocuous game like Candy Crush—you have accumulated a substantial amount of intimate privacy data. Intimate data ranges from your location, to when you fall asleep, to even more closely guarded information like your menstrual cycle or sexual partners. And every day, this data is scraped, bought, and sold by

---

[2] Zuboff, Shoshana. "You Are the Object of a Secret Extraction Operation." *The New York Times* (Nov. 12, 2021) *available at* https://www.nytimes.com/2021/11/12/opinion/facebook-privacy.html.
[3] Hern, Alex. "Grindr fined £8.6m in Norway over sharing personal information," *The Guardian* (Jan. 26, 2021) *available at* https://www.theguardian.com/technology/2021/jan/26/grindr-fined-norway-sharing-personal-information.
[4] "Grindr shared information about users' HIV status with third parties." *The Guardian* (Apr. 3, 2018) *available at* https://www.theguardian.com/technology/2018/apr/03/grindr-shared-information-about-users-hiv-status-with-third-parties.
[5] Clarke, Laurie. "Interview - Law professor Danielle Citron: 'Privacy is essential to human flourishing,'" *The Guardian* (Oct. 2, 2022) *available at* https://www.theguardian.com/technology/2022/oct/02/danielle-citron-privacy-is-essential-to-human-flourishing.

data brokers to third parties. Beyond violating our privacy, this repurposing of our personal data undermines our security.[6]

4) **The California Consumer Privacy Act and the California Privacy Rights Act (CPRA).** In 2018, the Legislature enacted the CCPA (AB 375 (Chau, Chap. 55, Stats. 2018)), which gives consumers certain rights regarding their personal information, such as the right to: (1) know what personal information about them is collected and sold; (2) request the categories and specific pieces of personal information the business collects about them; and (3) opt out of the sale of their personal information, or opt in, in the case of minors under 16 years of age.

Subsequently, in 2020, California voters passed Proposition 24, the California Privacy Rights Act (CPRA), which established additional privacy rights for Californians. With the passage of the CCPA and the CPRA, California now has the most comprehensive laws in the country when it comes to protecting consumers' rights to privacy.

In addition, Proposition 24 created the California Privacy Protection Agency (Privacy Agency) in California, vested with full administrative power, authority, and jurisdiction to implement and enforce the CCPA and the CPRA. The Agency's responsibilities include updating existing regulations, and adopting new regulations.

To protect Californians from any future legislative efforts to weaken statutory protections in the CPRA, Proposition 24 provided that the CPRA's contents may be amended by a majority vote of the Legislature only if the amendments are consistent with and further the purpose and intent of the CPRA, which is to further protect consumers' rights, including the constitutional right of privacy.[7]

5) **Suggested Committee amendments.** The Committee amendments are largely intended to clarify that the collection of personal information for verification purposes must be strictly protected. Toward that end, the proposed amendments make the following changes:

Amendment #1: Adds definition of personal information and sensitive personal information that matches the definitions in the CCPA.

(c) "Personal information" and "Sensitive personal information" has the same meaning as defined in Civil Code Section 1798.140

Amendment #2: Clarifies that requiring the deletion and restrictions related to information that is collected for the purposes of verifying a user, is in keeping with Civil Code Section 1798.100(c), which limits a business' collection, use, retention, and sharing of a consumer's personal information to that which is reasonably necessary and proportionate to achieve the purposes for which the personal information was collected.

Amendment #3: Reduces the time that platforms can retain the verification data from 30 days to 48 hours.

---

[6] Powell, Catherine. "Data is the New Gold, But May Threaten Democracy and Dignity," *Council on Foreign Relations* (Jan. 5, 2023) *available at* https://www.cfr.org/blog/data-new-gold-may-threaten-democracy-and-dignity-0.

[7] Ballot Pamphlet. Primary Elec. (Nov. 3, 2020) text of Prop. 24, p. 74

22686. ***(a) In accordance with Civil Code § 1798.100(c)*** ~~A~~ ***a*** social media platform that authenticates the identity of a user shall delete any personal information submitted by the user to the social media platform for that purpose within ***48 hours*** ~~30 days~~ of ~~the date upon which~~ the social media platform ***authenticating***~~s~~ the user's identity.

Amendment #4: Protects the personal information collected and limits its use.

(b)(1) A social media platform shall not use the identification information provided by a user for the purpose of complying with this section for any purpose other than authenticating the user's identity.

(2) A social media platform shall protect any identification information provided by a user in compliance with this section using, at a minimum, the standard of the industry used to protect the confidential information of users.

Amendment #5: Allows for the collection of civil fines for violations of the provisions in the bill.

(b) A social media platform that violates this section shall be liable for a civil penalty not to exceed two thousand five hundred dollars ($2,500) for each violation, which may be assessed and recovered in an action brought in the name of the people of the State of California by the Attorney General, a district attorney, a city attorney, county counsel, or a city prosecutor. In addition, the court shall award a prevailing public prosecutor reasonable costs and attorney's fees. For purposes of this section, each item of personal information that is either retained, used, shared, sold or disclosed in violation of this section shall constitute a separate violation. The remedies provided by this section are in addition to the remedies or penalties available under all other laws of this state.

6) **Related legislation.** AB 1949 (Wicks, 2024) would prohibit a business from collecting the personal information of a consumer under 18 years of age unless the consumer, or the consumer's parent or guardian if under 13, affirmatively authorizes the collection. That bill is currently pending in the Appropriations Committee.

AB 3030 (Alanis, 2024) would require a covered platform that publishes or distributes "material harmful to minors"—defined as material that is indecent, obscene, or child pornography—to perform reasonable age verification methods and prevent access by minors to the materials. That bill is currently pending in the Appropriations Committee.

AB 1501 (Hoover, 2023) would have required a commercial entity that knowingly and intentionally publishes or distributes sexually explicit material on the internet from a sexually explicit website to use an age verification method that prevents minors from accessing sexually explicit material. The bill was referred to this committee but was not heard.

SB 1228 (Padilla, 2024) would require 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. That bill is currently pending in the Senate Appropriations Committee.

ARGUMENTS IN OPPOSITION:

Writing in opposition to the bill, a coalition of opponents, including TechNet and the California Chamber of Commerce argues:

> Responsible online services take seriously the role they play in ensuring that users' personal information is properly safeguarded. Such businesses use an array of tools and security protocols to prevent and mitigate unauthorized access by nefarious actors through data breaches. As you know, the government itself is frequently the target of data hacks as it collects and stores large volumes of data concerning its residents. It is a shared responsibility across all industries and organizations to remain vigilant and protect against the ever-evolving and advancing tactics bad actors use to circumvent protective measures.
>
> While seemingly well-intentioned, the bill would counterintuitively impose a data retention and purpose limitation for a social media platform that chooses to provide user authentication mechanisms to serve a business purpose.

REGISTERED SUPPORT / OPPOSITION:

Support

California Women's Law Center
Public Health Advocates

Opposition

ACLU California Action
California Chamber of Commerce
Computer & Communications Industry Association
Netchoice
Technet

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