



May 14, 2025

The Honorable Robert Rivas  
Assembly Speaker  
1021 O Street, Suite 8330  
Sacramento, CA 94249

The Honorable Mike McGuire  
Senate President Pro Tempore  
1021 O Street, Suite 8518  
Sacramento, CA 95814

**Re: Concerns with Legislature’s Approach to Young People’s Online Safety**

Dear Speaker Rivas and President Pro Tempore McGuire:

I write today on behalf of the Electronic Frontier Foundation, a San Francisco-based, non-profit organization that works to protect civil liberties in the digital age. EFF represents more than 30,000 active donors and members, including thousands of supporters in California. For nearly 35 years, our organization’s lawyers, technologists and activists have ensured that internet policy respects the privacy, expression and innovation rights of everyday people and particularly vulnerable populations, including young people, LGBTQ+ people, immigrants, and people seeking reproductive health care. Drawing on that expertise, we have grave concerns about the way the California legislature is approaching regulation of the ways that young people access and navigate online services.<sup>1</sup>

We recognize that many young people face real harms online, that families are grappling with how to deal with them, and that tech companies are not offering much help. Several problems that young people have always faced—bullying, manipulation, predation—are now also digital problems. The ubiquity of devices in modern life can make them particularly difficult to address. However, many of the legislature’s proposals miss the root of the problem; threaten to increase privacy and security harms to all internet users, including young people; and often give large online platforms—not parents, guardians, or young people themselves—more control to manipulate and pass judgment on what is acceptable content for Californians’ youth.

**Don’t Hand Big Tech More Power to Control Speech**

Large online platforms have not solved many of our online safety problems. However, setting up broad liability for online platforms when young people are harmed online, as is the case in legislation such as A.B. 2 and A.B. 3172 (2024), will mandate platforms to censor a vast amount of protected speech. Such liability will inevitably lead services to steer clear of allowing even remotely controversial topics, such as young people’s health, safety, and sexuality, because they may become the subject of debate.<sup>2</sup>

---

<sup>1</sup> This letter will mention specific bills recently under consideration by the Legislature for illustrative purposes, but our fundamental concern is with the years-long trend of similar approaches.

<sup>2</sup> Brody Levesque. “Chino Valley Unified School District set to ban LGBTQ+ books,” Los Angeles Blade, (Nov. 17, 2023), available at <https://www.losangelesblade.com/2023/11/17/chino-valley-unified-school-district-set-to-ban-lgbtq-books/>

Such proposals could, for example, allow anti-LGBTQ+ advocates to file lawsuits against services and to impose penalties on sites or posts about LGBTQ+ issues and rights. Those lawsuits would likely push online services to restrict access to medical, health, and sexual information that many LGBTQ+ young people need.

These proposals also closely resemble legislation in other states that California would find abhorrent. For example, the Texas legislature is currently advancing a bill prohibiting the posting or hosting of content that shares information about abortion and allowing residents to sue anyone that violates the law. The only difference between the Texas bill and several bills we have seen moving through the California legislature is the topic that is prohibited; they rely on the same legal theories and would have devastating effects.

### **Age Gating Risks Exacerbating Harms**

Similarly, bills like A.B. 1043, which unilaterally restrict access to online services based on age, risk broadly harming children rather than protecting them. Lawmakers continue to ignore that children have the same First Amendment rights as adults to speak online and to access others’ speech. The Supreme Court has been explicit that, save for specific content and contexts not relevant here, bedrock First Amendment principles apply to minors “[e]ven where the protection of children is the object.”<sup>3</sup> The First Amendment protects not only what children can hear, but also what they can say.<sup>4</sup> Although parents can restrict their children’s access to lawful speech, and distributors can decide that they will not provide certain speech to minors without parental consent, the First Amendment prevents the government from establishing such restrictive defaults.<sup>5</sup> Lawmakers must reject proposals that seek to violate young people’s First Amendment rights.

Even if such proposals were not unconstitutional, they are bad policy. Age is an imperfect measure for maturity. Young people who are the same age may show wildly different levels of maturity. Additionally, often the most vulnerable young people—such as those whose parents don’t support their sexuality or gender identity, or who may be put in a position where they are acting as parents to younger siblings—are forced to grow up the fastest.

---

<sup>3</sup> *Brown v. Entertainment Merchs. Ass’n*, 564 U.S. 786, 804–05 (2011) (invalidating California’s regulation of violent video games for minors); *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 212–13 (1975) (invalidating restriction on drive-in movies designed to protect children from nudity); *Reno v. ACLU*, 521 U.S. 844, 874 (1997) (invalidating statute prohibiting indecent communications available to minors online).

<sup>4</sup> See *Mahanoy Area Sch. Dist. v. B.L. by & through Levy*, 594 U.S. 180, 187 (2021).

<sup>5</sup> See *Brown*, 564 U.S. at 803–04.

If age is the only yardstick in the law for restricting content from app store users and all apps, the law will trample youths’ rights to access important information, engage with diverse ideas, and communicate freely.

And these sorts of communications have been a lifeline for countless teens. We have asked young people about what they gain from access to social media and they responded in the thousands that the online platforms and communities they frequent are among the safest spaces for them—online or in the real world.<sup>6</sup> Several said that online communities educated them about abuse in their own lives, or simply made them feel less alone in situations where their parents were not supportive. Young people told us that online platforms are the safest spaces for them, where they can say the things they can’t say in real life ‘for fear of torment.’<sup>7</sup>

These responses show the relationship between social media and young people’s mental health is far more nuanced than the generalized claim that it is harmful.<sup>8</sup> This is particularly true for LGBTQ+ teens.<sup>9</sup> While this positive sentiment from young people is not the only perspective on this issue, the clear message that these spaces have improved their mental health and given them a ‘haven’ to talk openly and safely deserves serious consideration. These experiences also reflect findings from other respected research.<sup>10</sup>

Similarly, age gating with parental permission raises concerns for youth, especially whether such policies could unintentionally out LGBTQ+ youth to unsupportive parents or how they would work for foster or emancipated youth.

### **Age Verification Hurts Privacy, Speech, Access, and Security**

Furthermore, feeling safe to speak up online, particularly if you’re in a dangerous situation, is easier when you know you can be anonymous.<sup>11</sup> This is another reason why

---

<sup>7</sup> Jason Kelley, “Thousands of Young People Told Us Why the Kids Online Safety Act Will be Harmful to Minors,” Electronic Frontier Foundation (March 15, 2024), available at <https://www.eff.org/deeplinks/2024/03/thousands-young-people-told-us-why-kids-online-safety-act-will-be-harmful-minors>

<sup>8</sup> Alice Marwick et al., “Child Online Safety Legislation: A Primer,” Center for Information Technology Policy (May 29, 2024), available at [https://assets.pubpub.org/lwcjmvq1/Child\\_Online\\_Safety\\_Legislation\\_wDOI-11716569855951.pdf](https://assets.pubpub.org/lwcjmvq1/Child_Online_Safety_Legislation_wDOI-11716569855951.pdf)

<sup>9</sup> Matthew Berger et al., “Social Media Use and Health and Well-being of Lesbian, Gay, Bisexual, Transgender, and Queer Youth: Systemic Review,” *Journal of Medical Internet Research* (September 21, 2022), available at <https://pmc.ncbi.nlm.nih.gov/articles/PMC9536523/>

<sup>10</sup> Emily A. Vogels and Risa Gelles-Watnick, “Teens and Social Media: Key Findings from Pew Research Center surveys,” Pew Research Center (April 24, 2023), available at <https://www.pewresearch.org/short-reads/2023/04/24/teens-and-social-media-key-findings-from-pew-research-center-surveys/>

<sup>11</sup> Adam Schwartz and Jason Kelley. “Age Verification Mandates Would Undermine Anonymity Online.” *Electronic Frontier Foundation*, (March 22, 2023), available at [www.eff.org/deeplinks/2023/03/age-verification-mandates-would-undermine-anonymity-online](http://www.eff.org/deeplinks/2023/03/age-verification-mandates-would-undermine-anonymity-online).

EFF opposes age verification requirements. Once users share personal information to verify their age, they have no way to be certain that the data they’re handing over is not going to be stored, reused by the website, or even shared or sold to third parties.

While some age verification mandates have limits on retention and disclosure of this data, significant risk remains. Users are forced to trust that the website they visit, or its third-party verification service—both of which could be fly-by-night companies with no published privacy standards—are following these rules. This is a fundamental problem with bills that explicitly or implicitly require age verification, such as last year’s A.B. 3080 and S.B. 976. Unsurprisingly, given the strong constitutional protections that allow people, including young people, to access information anonymously, federal courts have blocked age verification laws in Arkansas, California, Mississippi, Ohio, Texas, and Utah.

Additionally, age verification laws affect all users, not just young people. Despite legislators’ focus on youth, age verification exposes everyone who uses these services to privacy and security harms and stifles their access to protected online content. They require the collection and storage of sensitive personal data, which could be misused or inadvertently exposed.<sup>12</sup>

The methods used to verify age online have foundational flaws that are especially harmful to vulnerable communities. Typically, websites rely on three primary means of verifying age online: using data brokers’ profiles of users, facial recognition, or government-issued IDs. Data brokers amass vast dossiers on us without our knowledge or consent, and age-verification that relies on them fuels a surveillance industry that increasingly targets children. Facial recognition, on the other hand, has well-documented racial and gender biases and poses particular difficulties for identifying transgender and nonbinary individuals.<sup>13</sup> Government ID-based systems require users to upload highly sensitive documents, which not only shuts out Californians who lack ID for whatever reason, but ignores the ease with which minors can get around this verification, such as by surreptitiously borrowing a parent’s ID.

Device-based verification raises its own issues as well. This approach disregards the many nuanced and context-dependent ways in which people use digital tools—such as low-income households where families often use a single device. The resulting complications from these types of proposals disproportionately impact already marginalized communities. In our response to an inquiry by the New York State Attorney General, EFF has documented the shortcomings of every major age verification method,

---

<sup>12</sup> Joseph Cox, “ID Verification Service for TikTok, Uber, X Exposed Driver Licenses.” *404 Media*, 404 Media, (June 28, 2024), available at [www.404media.co/id-verification-service-for-tiktok-uber-x-exposed-driver-licenses-au10tix/](http://www.404media.co/id-verification-service-for-tiktok-uber-x-exposed-driver-licenses-au10tix/).

<sup>13</sup> Morgan Klaus Scheuerman, et. al. "How computers see gender: An evaluation of gender classification in commercial facial analysis services." *Proceedings of the ACM on Human-Computer Interaction* 3.CSCW (2019): 1-33.

underscoring how each approach sacrifices user privacy and opens the door to new forms of harm.<sup>14</sup>

### **Constitutional Issues Delay Progress**

Finally, many proposals EFF has analyzed—including S.B. 845 (2023) and S.B. 1444 (2024), the current S.B. 243, A.B. 1064, and A.B. 56—are laden with unconstitutional provisions that will be blocked by courts. These include conflicts with the First Amendment rights of internet users and online services, and with 47 U.S.C. § 230 (“Section 230”). Federal courts have recognized these conflicts in cases regarding state laws restricting young people’s use of online services and have blocked at least seven of them—including two enacted in California—on First Amendment grounds.

Thus, bills that raise these issues are highly likely to face litigation that takes years to take resolve or may never take effect at all.

### **A Better Direction**

There are better alternatives that we can pursue now. In fact, many of these approaches, such as data minimization, are already included in some of the very bills we have mentioned. These alternative approaches can help protect children against many of the harms that lawmakers raise concerns about without undermining their independence or compromising the free expression and privacy rights of all internet users. For example, a well-crafted privacy law that empowers individuals to control how their data is collected and used would be a crucial step in curbing many of these problems.

California is a national leader on privacy, but its regime still relies mostly on allowing people to opt-out of data collection that is happening by default. That’s a huge burden on families and young people. Limiting by default the amount of data that companies can collect, use, and share about all of us would limit the kinds of harmful targeting that fuels much of the worry in many studies, surveys, and news reports.

It’s important to acknowledge that issues like substance abuse, eating disorders, and depression are complex, and that there is not clear agreement on their causes or their solutions. However, one thing is clear: people don’t want themselves or their families bombarded with manipulative ads. This privacy-by-default approach returns agency and power to children and their families to make decisions that are right for them. This approach would address a large chunk of the problem, while buying time to consider these issues with the nuance they deserve.

---

<sup>14</sup> “EFF comments to NY AG on SAFE for Kids (Sept. 2024)” <https://www.eff.org/document/eff-comments-ny-ag-safe-kids-sept-2024>

EFF letter of concern re: Young People's Online Safety  
May 14, 2025  
Page 6 of 6

For these reasons, we express our fundamental concerns about the legislature's approach to regulating how children interact with the internet, both during this session and in past ones. We believe there are other alternatives and would discuss them with any lawmaker interested in exploring a different path forward. Thank you.

Sincerely,

A handwritten signature in black ink, appearing to read 'Hayley Tsukayama', with a long horizontal flourish extending to the right.

Hayley Tsukayama  
Associate Director of Legislative Activism  
Electronic Frontier Foundation

cc: Honorable Members of the Assembly and Senate