



Testimony of Kouri Marshall  
Director of State & Local Government Relations, Central US  
Chamber of Progress  
Re: H.F.2257: Minnesota Age-Appropriate Design Code Act

March 1, 2023

The Honorable Zack Stephenson, Chair  
House Committee on Commerce, Finance, and Policy  
State Office Building  
100 Dr. Martin Luther King Jr. Boulevard  
St. Paul, MN 55155

Dear Chair Stephenson and members of the Committee:

Thank you for the opportunity to submit testimony for the record regarding H.F. 2257. On behalf of the Chamber of Progress, a tech industry coalition promoting technology's progressive future, I write to urge you to **oppose H.F. 2257**, which would undermine its own goals by sacrificing user privacy and jeopardizing many of the safe tools and resources already available to children.

Our organization works to ensure that all Americans benefit from technological leaps. Our corporate partners include companies like Google and Amazon, but our partners do not have a vote on or veto over our positions.

We agree that protecting young people online is an important goal. In recent years, many platforms have heard the concerns from parents and researchers and have implemented new features to protect younger users. These new features include limiting notifications at night, restricting messaging from advertisers, and increasing protections for content uploaded by children.<sup>1</sup>

**This bill would sacrifice all users' privacy in the name of increased security.**

---

<sup>1</sup> <https://www.nytimes.com/2021/12/09/technology/apps-child-protection.html>



H.F. 2257 would require covered sites to “estimate the age of child users with a “reasonable level of certainty.” One of the only ways to estimate users’ ages with enough certainty to avoid liability under the bill would be to affirmatively verify it.

The de facto age verification requirement would likely result in covered entities extracting even more data about their users, in spite of the bill’s stated emphasis on data minimization and privacy principles. There is disagreement about the best methods for verifying users’ ages, but they could include techniques like facial recognition or other biometric scans. Even less-invasive methods, like requiring users to enter their birthdate or ID in order to enter a site, would still require widespread data collection. These techniques would have to be used for every user, not just children, resulting in increased data collection for everyone on the internet.

Age verification would be particularly harmful for anyone looking to browse anonymously. Journalists, whistleblowers, and anyone looking to participate in online discussions would be forced to disclose personal details so that platforms could apply appropriate settings under this bill. This would limit free expression for groups who need it most.

Regardless of the method, age verification would **result in more surveillance of users and more data collection in the pursuit of increased security.**

**This bill also forces platforms to decide what content is appropriate for child users of all ages.** This bill requires that covered platforms act in the “best interests” of child users and create a plan to “mitigate or eliminate” the risk of encountering “harmful, or potentially harmful, content,” without providing clear guidance about what that entails.

While these are important considerations, in practice, this requirement would make each site the arbiter of appropriate content for children of all age ranges and circumstances. Platforms would face difficult choices about what types of



content to consider “harmful”, making it difficult to implement. As Chloe Alteri, Policy Counsel for the Future of Privacy Forum, noted:

“Aggregating all children under 18 in a single group may cause issues in implementation because the developmental needs and maturity of teenagers are vastly different from those of elementary school age children.”<sup>2</sup>

In order to avoid liability, covered platforms could take a broad view of content considered harmful and censor it for anyone under the age of 18. This bill does not include instructions for how to treat users in different age groups, ignoring the differences in developmental needs. Covered platforms could be forced to block older teenagers from accessing developmentally appropriate information simply because it would be inappropriate for much younger children.

For example, resources for LGBTQ+ youth or other vulnerable groups looking for support could be removed because they would not be appropriate for all users under 18. Teens looking for information on reproductive or sexual health services, including abortion access or rape crisis centers, could be prevented from accessing information that would not be suitable for 5 year olds. Educational resources, including academic journals, news articles, or documentaries featuring graphic images or depictions of violence, could be blocked because they would not be appropriate for younger users, even if they would be useful for high school students.

At a time when books with LGBTQ+ themes are being banned from school libraries and people providing healthcare to trans children are being falsely accused of “grooming,” this bill could cut off another vital avenue of access to information for vulnerable youth.

---

2

<https://fpf.org/blog/california-age-appropriate-design-code-aims-to-address-growing-concern-about-childrens-online-privacy-and-safety/>



**Additionally, H.F. 2257’s requirements could end up discouraging the development of age-appropriate experiences like the products that exist today.**

For any website that is “likely to be accessed” by children, H.F. 2257 requires Internet services to create and deliver Data Protection Impact Assessments (DPIAs) each time the service creates a new product or function. The DPIA must describe the risks of “material detriment” to children. Because all websites could be accessed by a child and all websites carry a nonzero risk of harm to children, H.F. 2257’s DPIA requirements effectively chill Internet services from developing new products and features—even products and features that could materially benefit and improve safety for children—to avoid future litigation risks associated with their DPIAs.

Platforms have created many popular sites and features with children’s needs in mind. YouTube Kids, for example, is a parentally-supervised, curated experience for younger kids, which uses a combination of algorithms and manual curation to show only kid-friendly videos.<sup>3</sup> Instagram applies different rules for the types of content it recommends to 13 to 18 year olds and has introduced new settings that give teens and parents more control over potentially upsetting content.<sup>4</sup> These features and sites are specifically designed to protect kids—with a more curated environment and content that has been vetted more than it would be for an adult audience.

With H.F. 2257 in place, before platforms developed these products, they would be forced to lay out all the potential risks to children and their plans to mitigate those risks. Because there is no way to completely eliminate harm, platforms would be setting themselves up for accusations of knowingly creating harmful products. To avoid that risk, **platforms might opt not to create features for children at all, resulting in children using less-curated sites or being blocked from platforms altogether.**

---

<sup>3</sup> [https://www.youtube.com/intl/ALL\\_us/kids/safer-experience/](https://www.youtube.com/intl/ALL_us/kids/safer-experience/)

<sup>4</sup> <https://about.instagram.com/community/parents#guide>



We agree with the need to build in greater protections for young users, but some of this bill's requirements would undermine the protections it tries to create and would end up harming vulnerable users.

Thank you,

**Kouri Marshall**

Director of State & Local Government Relations, Central US