



March 8, 2023

The Honorable Melony Griffith
Chair, Finance Committee
Miller Senate Office Building
11 Bladen Street
Annapolis, MD 21401

The Honorable Katherine Klausmeier
Vice-Chair, Finance Committee
Miller Senate Office Building
11 Bladen Street
Annapolis, MD 21401

RE: Oppose MD SB 0844 (Consumer Protection - Online Products and Services - Children's Data)

Dear Chair Griffith and members of the committee:

Thank you for the opportunity to submit testimony for the record regarding SB 0844. On behalf of Chamber of Progress, a tech industry coalition promoting technology's progressive future, I urge you to oppose SB 0844, which would undermine its own goals by sacrificing user privacy and jeopardizing many of the safe tools and resources already available to children.

We urge your committee to issue an unfavorable report on SB 0844 for several reasons. First, the age verification requirements would sacrifice all users' privacy in the name of increased security. Second, forcing platforms to decide what content is appropriate for all child users could result in over-removal of information. Third, the data protection impact assessment, or DPIA, could chill development of new products and features that could improve safety for children.

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.¹

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



First, this bill would sacrifice all users' privacy in the name of increased security. SB 0844 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.

De facto age verification requirements would likely result in covered entities extracting even more data about their users. 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.**

Second, this bill also forces platforms to decide what content is appropriate for all age ranges of minor users. This bill requires that covered platforms act in the “best interests” of child users and reduce their risk of encountering “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 every minor user.

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.”²

Platforms would face difficult choices about what types of content to consider “harmful” for every particular age group. 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. 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. 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.
- 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.

Third, the data protection impact assessment, or DPIA, could chill the development of new products and features that could improve safety for children, while also violating the First and Fourth Amendments.

2

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



For any website that is 'likely accessible' to children, the AADC requires Internet services to create and deliver Data Protection Impact Assessments (DPIA) to the Maryland AG's office each time the service creates a new product or function that is 'likely accessible to children.' The DPIA must describe the risks of 'material detriment' to children and state whether the product, feature, or service could 'harm' children.

Because all websites could be accessed by a child and all websites carry a nonzero risk of harm to children, the AADC's DPIA requirements could 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. As mentioned earlier, YouTube Kids uses a combination of algorithms and manual curation to show only kid-friendly videos.³ 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.⁴ 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.

Under a DPIA requirement, platforms 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.

Additionally, the Data Protection Impact Assessment (DPIA) requirements likely violate the First and Fourth Amendments of the U.S. Constitution – an issue which is the subject of a lawsuit challenging California's age appropriate design code.

³ https://www.youtube.com/intl/ALL_us/kids/safer-experience/

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



The AADC enables illegal searches by the State without cause, by requiring Internet companies to turnover their DPIAs to the State at any time without due process of law. This also enables the State to unconstitutionally inquire about the Internet service's editorial practices.

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,

Alain Xiong-Calmes

Chamber of Progress

Director of State & Local Government Relations, Northeast US